Recording Component (RC-P)

User Manual

© 2012 On-Net Surveillance Systems Inc.

On-Net Surveillance Systems, Inc.
One Blue Hill Plaza, 7th Floor, PO Box 1555
Pearl River, NY 10965
Phone: (845) 732-7900 | Fax: (845) 732-7999
Web: www.onssi.com

000051911-1653-RC-P1.0-OC3.0(3.0.3.250)

Legal Notice
This product manual is intended for general information purposes only, and due care has been taken in its preparation.

Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty.

© 2002-2012 On-Net Surveillance Systems, Inc. All rights reserved. OnSSI and the 'Eye' logo are registered trademarks of On-Net Surveillance Systems, Inc. Ocularis, Ocularis Client, Ocularis Client Lite, Ocularis Video Synopsis, NetEVS, NetDVMS, NetDVR, ProSight, NetGuard, NetGuard-EVS, NetSwitcher, NetMatrix, NetCentral, NetTransact, NetPDA and NetCell are trademarks of On-Net Surveillance Systems, Inc. All other trademarks are property of their respective owners.

On-Net Surveillance Systems, Inc. reserves the right to change product specifications without prior notice.

Patents Applied For in the U.S. and Abroad

Table Of Contents

System & Requirements 1
System Overview 1
Several Targeted Components in One 1
Updates 1
Minimum System Requirements 2
Administrator Rights 2
Important Port Numbers 3
Virus Scanning Information 3
Time Server Recommended 3
Installation 4
Installation 4
Upgrade 4
Upgrade from a Previous Version 4
Getting Started 6
Features 6
Get Your System Up and Running 6
Access the Management Application 7
Use the Built-in Help System 7
Navigating the Built-in Help System 8
Printing Help Topics 8
Wizards 9
Overview of Wizards 9
Configuration & Properties 10
Archiving Extends Recording Storage 10
Storing Archives at Other Locations than the Default Archiving Directory 10
Dynamic Path Selection for Archives 11
Archiving Audio 11
Different Drives: Automatic Archiving if Database Drive Runs Out of Disk Space 12
Same Drive: Automatic Moving or Deletion of Archives if Running Out of Disk Space 12
Archives Stored Locally 13
Exported Archives 13
Configure Archiving Locations 14
Configure Archiving Schedules 14
Audio 15
Add Audio Sources 15
Add Audio Sources 15
Configure Microphones 15
Microphone (Properties) 15
Cameras & Recordings 16
Add Cameras & Other Hardware Devices 16
Configure Video & Recording 16
View Video from Cameras in the Management Application 17
Configure When Cameras Should Do What 17
Monitor Storage Space Usage 17
Database Resizing 17
Disable or Delete Cameras 17
Wizards 18
Configure Video & Recording Wizard 18
Adjust Motion Detection Wizard 18
General Recording & Storage Properties 19
Recording & Archiving Paths 19
Dynamic Path Selection 19
Video Recording 20
Manual Recording 21
Frame Rate - MJPEG 22
Frame Rate - MPEG 23

Audio Selection 24
Audio Recording 25
Storage Information 25
Camera-Specific Properties 26
Camera 26
Frame Rate 26
Video 27
Audio 27
Recording Settings 27
Recording & Archiving Paths 28
Event Notification 29
Output 30
Motion Detection & Exclude Regions 30
PTZ Preset Positions 32
PTZ on Event 34
Events, Input & Output 35
Overview of Events, Input & Output 35
Configure General Event Handling 36
Add a Hardware Input Event 36
Add a Manual Event 37
Add a Timer Event 37
Add a Hardware Output 38
Configure Hardware Output on Event 38
General Event Properties 39
Ports & Polling 39
Event- & Output-Specific Properties 40
Hardware Input Event 40
Manual Event 40
Timer Event 41
Hardware Output 41
Hardware Devices 42
Add Hardware Devices 42
Configure Hardware Devices 42
Use Dedicated Input/Output Devices 43
Replace Hardware Devices 43
Delete Hardware Devices 43
Add Hardware Devices Wizard 44
Express Method 44
Advanced Method 44
Manual Method 44
Import from CSV File Method 44
Cameras and Server Are Online 45
Camera and Server Are Offline 45
Optional Parameters 45
Replace Hardware Device Wizard 47
Properties: Name & Video Channels 47
Network, Device Type & License 48
PTZ Device 48
Licenses 50
Import DLKs (Device License Keys) 50
Specify a New SLC (Software License Code) 50
Ocularis Base SLC 50
Recording Component (RC-P) SLC 50
Logging 51
Overview of Logs 51
Configure System, Event and Audit Logging 52
Properties: Logs 52
Management Application 54

Apply or Save Configuration Changes....54
Change or Reset Management Application Behavior....54
Configure the Management Application Password Protection....55
Scheduling....56
Configure General Scheduling and Archiving....56
Configure Camera-specific Schedules....56
General Scheduling Properties....57
Scheduling All Cameras....57
Scheduling Options....57
Archiving....58
Camera-specific Scheduling Properties....58
Online Period....58
Speedup....59
E-Mail Notification....60
Services....61
Overview of Services....61
Start & Stop Services....61
System....62
Configure Default File Paths....62
Find Version & Plug-in Information....62
System Restoration....63
Restore System Configuration from a Restore Point....63
Export & Import System Configuration....63
Import Changes to Configuration....64
Daylight Savings Time....68
Spring: Switch from Standard Time to DST....68
Fall: Switch from DST to Standard Time....68
Stability Improvement....69
Adding the 3 GB Switch....69
Removing the 3 GB Switch....70
Adding the 3 GB Switch....70
Removing the /3GB Switch....70
Protect Recording Databases from Corruption....70
Users....72
Overview of Users and Groups....72
Configure User Access Wizard....72
Add Basic Users....72
Add Windows Users....73
Add User Groups....73
Configure User and Group Rights....74
User Information....74
Group Information....74
General Access....74
Camera Access....74
Drivers....76
Update Video Device Drivers....76
Hardware Driver IDs....76
Ancillary Applications....80
Ocularis Client....80
NVR Download Manager....80
Using the NVR Download Manager....80
Initial Look....81
Installing New Features on Server....81
Making New Features Available through the Download Manager....81
Recording Server Manager....83
Using the Recording Server Manager....83
Ocularis Viewer....85
Backup....86
System Configuration Backup....86

To Back Up: *86*
To Restore Your Backed-up Configuration: *86*
Removal **87**
Entire System 87
Remove Entire Surveillance System *87*
Individual Components 87
Remove Installation Files for End-User Features *87*
Remove the NVR Download Manager 87
Remove the Surveillance Server Software 87
Remove Video Device Drivers 88
Contact Information **89**

System & Requirements

System Overview

The RC-P recording component is:

- *Compatible* with a wide range of different IP video products from the leading manufacturers, so you choose the hardware you want—in combinations too
- *Dependable*; with robust and stable performance proven in operation on thousands of cameras worldwide
- *Flexible*; with remote access features that let you use the surveillance system from any place and at any time
- *Scalable*; with open architecture based on IP technology with ongoing development and regular updates, which gives you long-term returns on your surveillance investment
- *Future-safe*; the IP network approach is the foundation for tomorrow—available today

Several Targeted Components in One

RC-P consists of a number of components, each targeted at specific tasks and user types:

- **The Management Application:** The main application used by surveillance system administrators for configuring the RC-P surveillance system server, upon installation or whenever configuration adjustments are required, for example when adding new cameras or users to the system.
- **The Recording Server service:** A vital part of the surveillance system; video streams are only transferred to RC-P while the Recording Server service is running. The Recording Server service is automatically installed and runs in the background on the RC-P surveillance system server. You can manage the service through the Management Application.
- **The Image Server service:** Handles access to the surveillance system for users logging in with clients. The Image Server service is automatically installed and runs in the background on the RC-P surveillance system server. You can manage the service through the Management Application.
- **The Download Manager:** Lets you manage which RC-P-related features your organization's users will be able to access from a targeted welcome page on the surveillance system server.
- **The Ocularis Client:** The Ocularis Client let users view live video, play back recorded video, activate output, print and export evidence, etc. The feature-rich Ocularis Client should always be downloaded and installed on remote users' computers.

Updates

On-Net Surveillance Systems, Inc. regularly releases service updates for our products, offering improved functionality and support for new devices. If you are a surveillance system administrator, it is recommended that you check www.onssi.com for updates at regular intervals in order to make sure you are using the most recent version of your surveillance software.

Minimum System Requirements

The following are *minimum* system requirements for running RC-P and associated applications. Visit the On-Net Surveillance Systems, Inc. website, www.onssi.com, for the most recent system performance parameters.

- ### RC-P Server

Operating System	Microsoft® Windows® Server 2003 (32 bit or 64 bit*), Windows Server 2008 R1/R2 (32 bit or 64 bit*).
CPU	Intel® Pentium® 4, 2.4 GHz or higher (Core™ 2 recommended).
RAM	Minimum 2 GB.
Network	Ethernet (1 Gbit recommended).
Hard Disk Type	E-IDE, PATA, SATA, SCSI, SAS (7200 RPM or faster).
Hard Disk Space	Minimum 1 GB free hard disk space available, excluding space needed for recordings.
Software	Microsoft .NET 3.5 Framework Service Pack 1 or newer. DirectX 9.0

***** Running as a 32 bit service/application.

- ### Ocularis Client

Operating System	Microsoft Windows XP Professional, Windows Vista Business, Ultimate, Enterprise (32 bit or 64 bit), Windows 7 Professional, Ultimate, Enterprise (32 bit or 64 bit).
CPU	Intel Core2™ Duo, minimum 2.4 GHz or higher (more powerful CPU recommended when running high number of cameras and multiple views and displays).
RAM	Minimum 2 GB (higher RAM recommended when running high number of cameras and multiple views and displays).
Graphics Adapter	PCI-Express, minimum 256 MB RAM, Direct 3D supported.
Software	Microsoft .NET 3.0 Framework Service, DirectX 9.0 or newer.

Administrator Rights

When you install RC-P it is important that you have administrator rights on the computer that will run RC-P. If you only have standard user rights, you will not be able to configure the surveillance system.

Consult your IT system administrator if in doubt about your rights.

Important Port Numbers

RC-P uses particular ports when communicating with other computers, cameras, etc.

What is a port? A port is a logical endpoint for data traffic. Networks use different ports for different types of data traffic. Therefore it is sometimes, but not always, necessary to specify which port to use for particular data communication. Most ports are used automatically based on the types of data included in the communication. On TCP/IP networks, port numbers range from 0 to 65536, but only ports 0 to 1024 are reserved for particular purposes. For example, port 80 is used for HTTP traffic when viewing web pages.

When using RC-P, make sure that the following ports are open for data traffic on your network:

- **Port 20 and 21 (inbound and outbound):** Used for FTP traffic. FTP (File Transfer Protocol) is a standard for exchanging files across networks. FTP uses the TCP/IP standards for data transfer, and is often used for uploading or downloading files to and from servers.
- **Port 25 (inbound and outbound):** Used for SMTP traffic. SMTP (Simple Mail Transfer Protocol) is a standard for sending e-mail messages between servers. This port should be open since, depending on configuration, some cameras may send images to the surveillance system server via e-mail.
- **Port 80 (inbound and outbound):** Used for HTTP traffic between the surveillance server and cameras, Ocularis Client, and the default communication port for the surveillance system's Image Server service. HTTP (HyperText Transfer Protocol) is a standard for exchanging files across networks; widely used for formatting and transmission of data on the world wide web.
- **Port 554 (inbound and outbound):** Used for RSTP traffic in connection with H.264 video streaming.
- **Port 1024 and above (outbound only):** Used for HTTP traffic between cameras and the surveillance server.
- Any other port numbers you may have selected to use, for example if you have changed the server access port from its default port number (80) to another port number.

Consult the administrator of your organization's firewall if in doubt about how to open ports for traffic.

Virus Scanning Information

Virus scanning on the RC-P server, and computers to which data is archived, should if possible be avoided:

- If you are using virus scanning software on the RC-P server, or on a computer to which data is archived, it is likely that the virus scanning will use a considerable amount of system resources on scanning all the data which is being archived. This may affect system performance negatively. Also, virus scanning software may temporarily lock each file it scans, which may further impact system performance negatively.
- Likewise, virus scanning software on the RC-P server is likely to use a considerable amount of system resources on scanning data used by the Download Manager.

If allowed in your organization, you should therefore disable any virus scanning of affected areas (such as camera databases, etc.) on the RC-P server as well as on any archiving destinations.

Time Server Recommended

All images are time-stamped by RC-P upon reception, but since cameras are separate units which may have separate timing devices, power supplies, etc., camera time and RC-P system time may not correspond fully, and this may occasionally lead to confusion.

If supported by your cameras, we recommend you auto-synchronize camera and system time through a time server for consistent synchronization.

For information about configuring a time server searching www.microsoft.com for *time server*, *time service*, or similar.

Installation

Installation

Do not install RC-P on a mounted drive (that is a drive attached to an empty folder on an NTFS (NT File System) volume, with a label or name instead of a drive letter). If using mounted drives, critical system features may not work as intended; you will, for example, not receive any warnings if the system runs out of disk space.

Prerequisites: Shut down any existing surveillance software. If upgrading, read Upgrade from a Previous Version first.

1. Insert the RC-P software DVD, wait for a short while, click the RC-P installation link, then select required language.

   Alternatively, if you are installing a version downloaded from the internet, run the downloaded installation file from the location you have saved it to.

   Depending on your security settings, you may receive one or more security warnings (such as *Do you want to run or save this file?*, *Do you want to run this software?* or similar). When this is the case, click the *Run* button.

2. When the installation wizard starts, click *Next* to continue.

3. Read and accept the End User License Agreement, then click *Next*.

4. If an earlier RC-P version is present on the server, you will be asked to accept that it is automatically removed during installation of the new version. The automatic removal will not delete any existing recordings or configuration. If asked, we recommend answering *Yes*, since this will ensure that old versions will not interfere with your new version.

5. Select *Typical* installation (advanced users may select *Custom* installation, and choose which features to install and where to install them).

6. Select *Install licensed version*. Specify your user name, organization, and Software License Code (SLC). When ready, click *Next*.

7. Click the *Install* button to begin the software installation. During the process, all the necessary components will be installed one after the other.

8. Click *Finish* on the last step to complete the installation.

   - If a *Status Information* window appears on your screen during installation, simply click its *OK* button. The window simply provides a summary of your installation.

When installation is complete, you can begin configuring RC-P through the *Management Application*: Double-click the Management Application desktop shortcut or select *Start > All Programs > OnSSI > Management Application*. See more under Get Your System Up & Running.

Upgrade

Upgrade from a Previous Version

Upgrading from one RC-P version to another RC-P version is an easy task, and you need not worry about spending hours reconfiguring your software.

- #### Prerequisites
  - Take note of your SLC (Software License Code). The SLC will change when the software version number changes.
  - If your SLC has changed, so have your DLKs (Device License Keys). You get DLKs (Device License Keys) upon request. Once approved, all your DLKs are sent to you as a single .dlk file attached to an e-mail. When you have installed the new version of RC-P, you should import the new DLK file as described later.

- #### Back Up Your Current Configuration

  When you install the new version of RC-P, it will inherit the configuration from your old version.

However, we recommend that you make regular backups of your server configuration as a disaster recovery measure. Upgrading your server is no exception. While it is rare to lose your configuration (cameras, schedules, views, etc), it *can* happen under unfortunate circumstances. Luckily, it takes only a minute to back up your existing configuration:

1. Create a folder called *Backup* on a network drive, or on removable media.
2. On the RC-P server, open *My Computer*, and navigate to C:\Program Files\OnSSI\RC-P.
3. Copy the following files and folders into your Backup folder:
    - All configuration (.ini) files
    - All scheduling (.sch) files
    - The file *users.txt* (only present in a few installations)

- ### Remove the Current Version

  In most cases, you do not need to manually remove the old version of RC-P before you install the new version. The old version is removed when you install the new version.

- ### Install the New Version

  Run the installation file for the new software version. Select the installation options that best fit your needs.

- ### Import New DLKs

  1. Open the Management Application.
  2. In the Management Application's *File* menu, select *Import DLKs...*
  3. Browse to the location at which you have saved the received .dlk file, select the file, and click *Open*. All the new DLKs are now imported into RC-P.

- ### Upgrade Video Device Drivers

  Video device drivers are small programs used for controlling/communicating with the hardware devices connected to an RC-P system.

  Video device drivers are installed automatically during the installation of your RC-P system. However, new versions of the video device drivers—also called Device Packs—are released and made available for from time to time.

  We therefore recommend that you regularly visit the OnSSI website (look under *Support > Downloads, Demos, Manuals, Tutorials & White Papers*) and download the latest Device Pack.

  When updating video device drivers, there is no need to remove the old video device drivers first; simply install the latest version on top of any old version you may have. For detailed information, see Update Video Device Drivers.

- ### Upgrade Ocularis Clients

  Ocularis Client users should remove their old Ocularis Client versions and install the new one:

  1. On the required computers, open a browser and connect to RC-P at the following address:

     http://[IP address or hostname of server]:[port number; default is 80]

     Example: http://123.123.123.123:80

  2. From the welcome page that appears, download and install the latest Ocularis Client version.

  The installation wizard will prompt you to uninstall any older versions it may find.

Getting Started

Features

RC-P 1.0 contains many interesting and powerful features:

- **Single Management Application**. A single Management Application has a modern look and an intuitive and consistent grouping of features.
- **Wizard-driven configuration** guides you through common RC-P tasks, such as adding of hardware devices and cameras to the system. Detailed configuration, without wizards, is also possible.
- **Multi-instance configuration** through templates or quickly editable summaries lets you configure multiple cameras, events, users, etc. in one step.
- **No separate Image Server Administrator application**; all management of users, rights, etc. takes place directly in the Management Application.

Among the less noticeable—yet important—features you will find that:

- **Archiving takes place automatically**. See Archiving Extends Recording Storage.
- **You can view live video in the Management Application**. See View Video from Cameras in Management Application.
- **Configuration is stored as XML**. New upgrades easily maintain system configuration.
- **Configuration restore points** let you quickly return to a previous configuration state. See Restore System Configuration from Restore Point.
- **You can export and import configurations**, for example if installing many similar RC-P systems. See Export & Import System Configuration and Import Changes to Configuration.

Get Your System Up and Running

The following outlines the tasks typically involved in setting up a working RC-P system. Note that although information is presented as a checklist, a completed checklist does not in itself guarantee that the system will match the exact needs of your organization. To make the system match the needs of your organization, it is highly recommended that you monitor and adjust the system once it is running.

For example, it is often a very good idea to spend time on testing and adjusting the motion detection sensitivity settings for individual cameras under different physical conditions (day/night, windy/calm, etc.) once the system is running. The setup of events and associated actions typically also depends entirely on your organization's needs.

☐ **Verify Initial Configuration of Cameras and other Hardware Devices**
Before doing anything on RC-P, make sure the hardware devices (cameras, video encoders, etc.) you are going to use are correctly installed and configured with IP addresses, passwords, etc. as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the network and RC-P.

☐ **Register Your RC-P Software and Get DLKs**
You must register your software and get a Device License Key (DLK) for every device (cameras, etc.) you are going to use on your RC-P system. Upon request, all your DLKs are sent to you as a single .dlk file attached to an e-mail.

- Go to www.onssi.com and click the *Device Registration* link in the Support section.
- Fill out the *Software Registration and Device License Keys* form.
- Click *Send*.
- When processed by OnSSI, you will receive an email with an attachment. Detach this .dlk file and prepare to import it into RC-P.

☐ **Install the RC-P Recording Component**
See Install Surveillance Server Software. If upgrading an existing version of RC-P, see Upgrade from a Previous Version.

☐ **Open the Management Application**
See Access the Management Application.

☐ **Import Your DLKs**
Now it is time to import the Device License Keys into RC-P; see Import DLKs (Device License Keys).

☐ **Add Hardware Devices in RC-P** can quickly scan your network for relevant hardware devices (cameras, video encoders, etc.), and add them to your system. See Add Hardware Devices.

☐ **Configure Cameras in RC-P**
You can specify a wide variety of settings for each camera connected to your RC-P system. Settings include video format, resolution, motion detection sensitivity, where to store and archive recordings, any PTZ (Pan/Tilt/Zoom) preset positions, association with microphones, etc. See Configure Video & Recording Settings.

> **What does "... archive recordings" mean?** Archiving—an integrated and automated feature—helps you store recordings beyond the capabilities of RC-P's standard database. Archiving thus maximizes storage capacity and minimizes risk. See Archiving Extends Recording Storage.

☐ **Configure Scheduling**
When do you want to archive? Do you want some cameras to transfer video to RC-P at all times, and other cameras to transfer video only within specific periods of time, or when specific events occur? With the scheduling feature, you can specify this as well as when you want to receive notifications from the system. See Configure General Scheduling & Archiving and Configure Camera-specific Schedules.

☐ **Configure Users**
Now specify at least one user account for access your RC-P system. This user account should have full access rights to all devices and will be used to import the RC-P into Ocularis. See Quickly Add Users with Access to All Cameras, Add Individual Users, Add User Groups and Configure User & Group Rights.

☐ **Install Ocularis Base**
Proceed with the installation of the remaining Ocularis components and license Ocularis Base (if not already done). See the *Ocularis Installation and Licensing Guide* available in the installation package/DVD or from www.onssi.com.

☐ **Configure Ocularis Base**
Launch the Ocularis Administrator application to configure Oculars Base and import the RC-P Recording Component. See the *Ocularis Administrator's User Manual* for more details.

☐ **Configure Ocularis Client**
Install Ocularis Client (if you haven't already done so) and configure local settings. See the *Ocularis Client User Manual* for more details..

The above list represents the configuration steps that most administrators are likely to cover. Additional configuration is of course likely due, for instance, to continued tweaking of system settings for cameras and storage.

Note that the behavior of the Management Application can be customized. Descriptions here are, however, always based on the Management Application's default behavior.

Access the Management Application

You access the Management Application by double-clicking the *Management Application* desktop shortcut.

Alternatively, use Windows' *Start* menu: *Start* > *All Programs* > *OnSSI* > *Management Application*.

Depending on your configuration, access to the Management Application may be password-protected.

Use the Built-in Help System

To use RC-P's built-in help system, simply click the *Help* button in the Management Application's toolbar. Alternatively, press the F1 key on your keyboard while using RC-P.

The help system opens in a separate window, allowing you to easily switch between help and RC-P. The help system is context-sensitive. This means that when you press F1 for help while working in a particular RC-P dialog, the help system automatically displays help matching that dialog.

Navigating the Built-in Help System

To navigate between the help system's contents, simply use the help window's tabs: *Contents*, *Search*, *Favorites* and *Glossary,* or use the links inside the help topics.

- ***Contents Tab*:** Navigate the help system based on a tree structure. Many users will be familiar with this type of navigation from, for example, Windows Explorer.

- ***Search Tab*:** Search for help topics containing particular terms of interest. For example, you can search for the term *zoom* and every help topic containing the term *zoom* will be listed in the search results. Double-clicking a help topic title in the search results list will open the required topic.

- ***Favorites Tab*:** Build a list of your favorite help topics. Whenever you find a help topic of particular interest to you, simply add the topic to your favorites list. You can then access the topic with a single click—also if you close the help window and return to it later.

Help topics contain various types of links, notably so-called expanding drop-down links. Clicking such a link will display detailed information immediately below the link itself; the content on the topic simply expands. Expanding drop-down links thus help save space.

Printing Help Topics

To print a help topic, navigate to the required topic and click the help window's *Print* button. A dialog box may ask you whether you wish to print the selected topic only or all topics under the selected heading; when this is the case, select *Print the selected topic* and click *OK*.

Wizards

Overview of Wizards

Wizards guide you through common tasks in RC-P:

- The Add Hardware Devices wizard helps you add cameras and other hardware devices, such as video encoders, to your RC-P system. If microphones are attached to a hardware device, they are automatically added as well.
- The Configure Video and Recording wizard helps you quickly configure your cameras' video and recording properties.
- The Adjust Motion Detection wizard helps you quickly configure your cameras' motion detection properties.
- The Configure User Access Wizard helps you quickly configure clients' access to the RC-P server.

Configuration & Properties

Archiving Extends Recording Storage

Archiving is an integrated and automated feature that helps you store recordings beyond the capabilities of RC-P's standard database. Archiving maximizes storage capacity and minimizes risk; you can keep recordings for as long as required, limited only by the available hardware storage capacity.

In the following topics, archiving is explained in detail. If you want to configure archiving immediately, see Configure Archiving Locations and Configure Archiving Schedules.

- ### Benefits of Archiving

  With archiving, recordings are moved from their standard location to another location, the archiving location. With archiving, the amount of recordings you are able to store is limited only by the available hardware storage capacity:

  By default, recordings are stored in RC-P's database for each camera. The database for each camera is capable of containing a maximum of 600000 records or 40 GB.

  However, the maximum size of a database is not in itself very important: If a database for a camera becomes full, RC-P automatically begins archiving its content, freeing up space in the database. Having sufficient archiving space is more important (see Storage Capacity Required for Archiving in the following).

  In addition to automatic archiving when a database becomes full, you can schedule archiving to take place at particular times up to 24 times per day. This way, you can proactively archive recordings, so databases will never become full.

  By using archiving, you will also be able to back up archived records on backup media of your choice, using your preferred backup software.

- ### How Archiving Works

  For each camera, the contents of the camera database will be moved to a default archiving folder, called *Archives*. This will happen automatically if a database becomes full, and one or more times every day, depending on your archiving settings.

  The default archiving folder is located on the RC-P server, by default in C:\VideoData.

  In the archiving folder, separate subfolders for storing archives for each camera are automatically created. These subfolders are named after the MAC address of the hardware device to which the camera is connected.

  Since you can keep archives spanning many days of recordings, and since archiving may take place several times per day, further subfolders, named after the archiving date and time, are also automatically created.

  The subfolders will be named according to the following structure:

  ...\Archives\CameraMACAddress_VideoEncoderChannel\DateAndTime

  Example: With the default archiving folder located under C:\VideoData, video from an archiving taking place at 23.15 on 31st December 2010 for a camera attached to channel 2 on a video encoder hardware device with the MAC address 00408c51e181 would be stored at the following destination:

  C:\VideoData\Archives\00408c51e181_2\2010-12-31-23-15

  If the hardware device to which the camera is attached is not a video encoder device with several channels, the video encoder channel indication in the sub-directory named after the hardware device's MAC address will always be *_1* (example: 00408c51e181_1).

  #### Storing Archives at Other Locations than the Default Archiving Directory

  You may also store archives in other directories than the default archiving directory. However, you cannot archive to external drives, only to a local drive on the computer running RC-P.

Dynamic Path Selection for Archives

With dynamic archiving paths, you specify a number of different archiving paths, usually across several drives. Using dynamic paths is highly recommended, and is the default setting when you configure cameras through the Configure Video & Recording Wizard.

If the path containing the camera's database is on one of the drives you have selected for dynamic archiving, RC-P will always try to archive to that drive first. If not, RC-P automatically archives to the archiving drive with the most available space at any time, provided there is not a camera database using that drive.

Which drive that is used for archiving may change during the archiving process, and archiving may therefore happen to several archiving drives during the same process. This fact will have no impact on how users find and view archived recordings.

Dynamic archiving paths are general for all your cameras; you cannot configure dynamic archiving paths for individual cameras.

When deciding which drives to use for dynamic archiving, consider the pros and cons in the following examples (in which we assume that the default archiving path is on drive C:—drive letters are examples only, different drive letters may of course be used in your organization):

Camera records to drive C: and archives to drive C:
If the path containing the camera's database is on one of the drives you have selected for dynamic archiving, RC-P will always try to archive to that drive first. Archiving will take place quickly, but may also fairly quickly fill up the drive with data.

Camera records to drive C: and archives to drive D:
Obvious benefit is that recordings and archives are on separate drives. Archiving takes place less quickly. RC-P will first temporarily store the archive in the local default archiving directory on C:, then immediately move the archive to the archiving location on D:. Therefore, sufficient space to accommodate the temporary archive is required on C:.

Camera 1 records to drive C: and archives to drive D:
while
Camera 2 records to drive D: and archives to drive C:
Avoid. One camera's archiving may take up space required for another camera's recordings. In the above example, Camera 1's archiving to D: may result in no recording space for camera 2 on D:. The rule of thumb is: “Do not cross recording and archiving drives.”

Archiving Audio

If an audio source (microphone is enabled on a hardware device, audio recordings will be archived together with video recordings from the camera attached to the hardware device. If the hardware device is a video encoder with several channels, audio will be archived with the camera on channel 1.

When an audio source is enabled, audio is recorded to the associated camera’s database. This will affect the database’s capacity for storing video. You may therefore want to use scheduled archiving more frequently if recording audio *and* video than if only recording video.

Storage Capacity Required for Archiving

The storage capacity required for archiving depends entirely on the amount of recordings you plan to keep, and on how long you want to keep them (also known as retention time).

Some organizations want to keep archived recordings from a large number of cameras for several months or years. Other organizations may only want to archive recordings from one or two cameras, and they may want to keep their archives for much shorter periods of time.

You should always first consider the storage capacity of the **local** drive containing the default archiving directory to which archived recordings are always moved, even though they may immediately after be moved to an archiving location on another drive: As a rule of thumb, the capacity of the local drive should be at least twice the size required for storing the databases of all cameras.

You cannot archive to external drives, only to local drives on the RC-P server.

When archiving, RC-P automatically checks that space required for the data to be archived plus 1 GB of free disk space per camera is available at the archiving location. If not, the archive location's oldest data from the camera in question will be deleted until there is sufficient free space for the new data to be archived.

In short: When estimating storage capacity required for archiving, consider your organization's needs, then plan for worst case rather than best case scenarios.

- ## Automatic Response if Running Out of Disk Space

With archiving, RC-P can automatically respond to the threat of running out of disk space. Two scenarios can occur, depending on whether the camera database drive is different from, or identical to, the archiving drive:

Different Drives: Automatic Archiving if Database Drive Runs Out of Disk Space

In the case where the RC-P server is running out of disk space, and

- the archiving drive is ***different from*** the camera database drive, and
- archiving has not taken place within the last hour,

archiving will automatically begin in an attempt to free up disk space. This will happen regardless of any archiving schedules.

The server is considered to be running out of disk space if:

- there is less than 10% disk space left, and the available disk space goes below 30 GB plus 1.5 GB per camera

  - or -

- the available disk space goes below 150 MB plus 20 MB per camera (example: with ten cameras, the server would be running out of disk space if the remaining available disk space went below 350 MB (150 MB plus 20 MB for each of the ten cameras))

The difference ensures that very large disks will not necessarily be considered to be running out of disk space just because they have less than 10% disk space left.

On the archiving drive, RC-P automatically checks that the space required for data from a camera to be archived plus 1 GB of free disk space per camera is available. If not, the archive drive's oldest data from the camera in question will be deleted until there is sufficient free space for the new data to be archived.

IMPORTANT: You will lose the archive data being deleted.

Same Drive: Automatic Moving or Deletion of Archives if Running Out of Disk Space

In the case where the RC-P server is running out of disk space, and the archiving drive is ***identical to*** the camera database drive, RC-P will automatically do the following in an attempt to free up disk space:

1. First, RC-P will attempt to delete archives. This will happen if:
   - there is less than 10% disk space left, and the available disk space goes below 30 GB plus 1.5 GB per camera

     - or -

   - the available disk space goes below 150 MB plus 20 MB per camera (example: with ten cameras, the server would be running out of disk space if the remaining available disk space went below 350 MB (150 MB plus 20 MB for each of the ten cameras))

   The difference ensures that very large disks will not necessarily be considered to be running out of disk space just because they have less than 10% disk space left.

   IMPORTANT: You will lose data from the archives being deleted.

2. Ultimately, if there are no archives to delete, RC-P will attempt to resize camera databases. This will happen if:
   - there is less than 5% disk space left, and the available disk space goes below 20 GB plus 1 GB per camera

     - or -

   - the available disk space goes below 75 MB plus 10 MB per camera (example: with ten cameras, the server would be running out of disk space if the remaining available disk space went below 175 MB (75 MB plus 10 MB for each of the ten cameras))

   The difference ensures that very large disks will not necessarily be considered to be running out of disk space just because they have less than 5% disk space left.

   IMPORTANT: You will lose the data deleted as part of the database resizing process.

   When the recording server is restarted upon such database resizing, the original database sizes will be used. You should therefore make sure the drive size problem is solved, or adjust camera database sizes to reflect the altered drive size.

Tip: Should the database resizing procedure take place, you will be informed in log files, and (if set up) through an e-mail notification.

- ## Backing Up Archives

  Many organizations want to back up recordings from cameras, using tape drives or similar. Creating such backups based on the content of camera databases is not recommended; it may cause sharing violations or other malfunctions.

  Instead, create such backups based on the content of archives. If you have not specified separate archiving locations for separate cameras, you could simply back up the default local archiving directory, *Archives*. When scheduling a backup, make sure the backup job does not overlap with any scheduled archiving times.

- ## Viewing Archived Recordings

  Archived recordings may be viewed with the Ocularis Client. You are able to use all of Ocularis Client's advanced features (video browsing, searching, export, etc.) for archived recordings as well.

  ### Archives Stored Locally

  For archived recordings stored locally you simply use the Ocularis Client's playback features, for example the Kinetic Timeline browser, for finding and viewing the required recordings; just like you would with recordings stored in a camera's regular database.

  ### Exported Archives

  For exported archives, for example archives stored on a CD, you may also use the Ocularis Client.

- ## Virus Scanning and Archiving

  If allowed in your organization, disable any virus scanning of camera databases and archiving locations. For more information see Virus Scanning Information.

- ## New Database if Archiving Fails

  Under extremely rare circumstances archiving may fail. For example, a database may be full and ready for archiving, but the operating system may lock content in the database if a content file is open. This would prevent archiving. In practice, this situation would only occur if somebody attempted to view a database file directly from the database folder at the time of the archiving (viewing the file directly would actually not work since database content cannot be viewed as individual files, only through the Ocularis Client).

  In such situations, the database will be put aside for archiving at a later point in time. While the database is put aside, a special temporary database is created for storage of new recordings. This way, no new recordings will be lost even though the original database is full (provided enough disk space is available for storing the special temporary database).

  RC-P will wait for the next archiving occasion (either scheduled or because the special temporary database also becomes full). It will then archive the content of the special temporary database, and thus free up space in it. RC-P will then continue to store new recordings in the special temporary database. This will apply until the Recording Server service is restarted. Once the service has been restarted, the content of the original database will be archived, and new recordings will again be stored in the original database. The special temporary database will also be archived, and will then cease to exist.

  Can I view recordings from the special temporary database? Normally, the content of databases can be viewed with the Ocularis Client regardless whether the databases have been archived or not. However, the content of the special temporary database cannot be viewed through a client until the content has been archived. On the surveillance server itself, you will be able to view the content of the special temporary database through the Ocularis Client, even if the special temporary database has not been archived yet. Since the special temporary database will be used for storing new recordings until the Recording Server service is restarted—even though the original database may no longer be locked—you may in these extremely rare situations experience that new recordings are not viewable through clients. In that case, restarting the Recording Server service will help, since it will force the original database to again be used for storing new recordings.

Configure Archiving Locations

Before configuring archiving locations, consider whether you want to use static or dynamic archiving paths:

- **Static** archiving paths mean that for a particular camera, archiving will take place to a particular location, and to that location only. Static archiving paths are in principle individual for each camera, but they do not have to be unique: several cameras can easily use the same path if required.

  You can configure static archiving paths for individual cameras, or as part of the general Recording & Archiving Paths properties.

  - **Individual cameras:** In the Management Application's navigation pane, expand *Advanced Configuration*, expand *Cameras and Storage Information*, double-click the required camera, select *Recording & Archiving Paths*, and specify required properties.

  - **General Recording & Archiving Paths:** In the Management Application's navigation pane, expand *Advanced Configuration*, double-click *Cameras and Storage Information*, and specify required properties.

- **Dynamic** archiving paths allow greater flexibility, and are therefore highly recommended. With dynamic archiving paths, you specify a number of different archiving paths, usually across several drives.

  If the path containing the camera database to be archived is on one of the drives you have selected for dynamic archiving, RC-P will always try to archive to that drive first. If not, RC-P automatically archives to the archiving drive with the most available space at any time, provided there is not a camera database using that drive. This fact will have no impact on how users find and view archived recordings.

  Dynamic archiving paths are general for all your cameras; you cannot configure dynamic archiving paths for individual cameras.

  To configure archiving paths: In the Management Application's navigation pane, expand *Advanced Configuration*, double-click *Cameras and Storage Information*, select *Dynamic Path Selection - Archives*, and specify required properties.

If configuring your cameras through the Configure Video & Recording Wizard, the wizard also lets you configure archiving paths.

Configure Archiving Schedules

RC-P automatically archives recordings if a camera's database becomes full (in earlier versions, this was an option configured individually for each camera).

You are furthermore able to schedule archiving at particular points in time up to 24 times per day, with minimum one hour between each one. This way, you can proactively archive recordings, so databases will never become full. As a rule of thumb, the more you expect to record, the more often you should archive.

There are two ways in which to configure archiving schedules:

- While configuring your cameras through the Configure Video & Recording Wizard, in which case you configure your archiving schedule on the wizard's *Drive selection* page.

- As part of the general Scheduling & Archiving Paths properties: In the Management Application's navigation pane, expand *Advanced Configuration*, right-click *Scheduling and Archiving*, select *Properties*, select *Archiving* in the dialog, and specify required properties.

Audio

Add Audio Sources

You add cameras and other hardware devices, such as video encoders, to your RC-P system through the Add Hardware Devices... wizard. If microphones are attached to a hardware device, they are automatically added as well.

When managing microphones in RC-P, it is important to remember the basic concepts:

- **Microphones** are attached to hardware devices, and are typically physically located next to cameras. They generally record what people near a camera are saying. Operators, with the necessary rights, can then listen to these recordings through their Ocularis Client (provided the computer running the Ocularis Client has speakers attached). In RC-P it is only possible to have one microphone enabled at a time.

Add Audio Sources

You add cameras and other hardware devices, such as video encoders, to your RC-P system through the Add Hardware Devices... wizard. If microphones are attached to a hardware device, they are automatically added as well.

When managing microphones in RC-P, it is important to remember the basic concepts:

- **Microphones** are attached to hardware devices, and are typically physically located next to cameras. They generally record what people near a camera are saying. Operators, with the necessary rights, can then listen to these recordings through their Ocularis Client (provided the computer running the Ocularis Client has speakers attached). In RC-P it is only possible to have one microphone enabled at a time.

Configure Microphones

Configuration of microphones in RC-P is very basic; settings such as volume, etc. are controlled on the microphone units themselves.

1. In the Management Application's navigation pane, expand *Advanced Configuration*, expand *Hardware Devices*, and expand the hardware device to which the required microphone is attached.
2. Right-click the required microphone, and select *Properties*.
3. Specify properties as required.
4. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

Microphone (Properties)

When you configure microphones, properties are limited to:

- ***Enabled*:** Microphones are by default enabled, meaning that they are able to transfer audio to RC-P. If required, you can disable an individual microphone, in which case no audio will be transferred from the microphone to RC-P.
- ***Microphone name*:** Name of the microphone as it will appear in the Management Application as well as in clients. If required, you can overwrite the existing microphone name with a new one. Microphone names must be unique, and must not contain any of the following special characters: < > & ' " \ / : * ? | [ ]

In RC-P it is only possible to have one microphone enabled at a time.

On some hardware devices, audio can also be enabled/disabled on the hardware device itself, typically through the hardware device's own configuration web page. If audio on a hardware device does not work after enabling it in the Management Application, you should thus verify whether the problem may be due to audio being disabled on the hardware device itself.

Cameras & Recordings

Add Cameras & Other Hardware Devices

You add cameras and other hardware devices, such as video encoders, to your RC-P system through the Add Hardware Devices... wizard. If microphones are attached to a hardware device, they are automatically added as well.

The wizard offers you four different ways of adding cameras:

- **Express (recommended):** Scans your network for relevant hardware devices, and helps you quickly add them to your system. To use the Express method, your RC-P server and your cameras must be on the same layer 2 network, that is a network where all servers, cameras, etc. can communicate without the need for a router. See Add Hardware Devices Wizard - Express.

- **Advanced:** Scans your network for relevant hardware devices based on your specifications regarding required IP ranges, discovery methods, drivers, and device user names and passwords. See Add Hardware Devices Wizard - Advanced.

- **Manual:** Lets you specify details about each hardware device separately. A good choice if you only want to add a few hardware devices, and you know their IP addresses, required user names and passwords, etc. See Add Hardware Devices Wizard - Manual.

- **Import from CSV file:** Lets you import data about cameras as comma-separated values from a file; an effective method if setting up several similar systems. See Add Hardware Devices Wizard - Import from CSV File.

Configure Video & Recording

Once you have added hardware devices and attached cameras, you can configure video and recording settings in three ways:

- **Wizard-driven:** Guided configuration which lets you specify video, recording and archiving settings for all your cameras. See Configure Video & Recording Wizard and Adjust Motion Detection Wizard.

- **General:** Lets you specify video, recording and shared settings (such as dynamic archiving paths and whether audio should be recorded or not) for all your cameras.

    1. In the Management Application's navigation pane, expand *Advanced Configuration*, right-click *Cameras and Storage Information*, and select *Properties*.

    2. Specify properties as required for Recording & Archiving Paths, Dynamic Path Selection, Video Recording, Frame Rate - MJPEG, Frame Rate - MPEG, Audio Selection, and Audio Recording. When ready, click *OK*.

    3. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

- **Camera-specific:** Lets you specify video, recording and camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for each individual camera.

    1. In the Management Application's navigation pane, expand *Advanced Configuration*, and expand *Cameras and Storage Information*.

    2. Right-click the required camera, and select *Properties*.

    3. Specify properties as required for Camera, Frame Rate, Video, Audio, Recording, Recording & Archiving Paths, Event Notification, Output, Motion Detection & Exclude Regions, and—if applicable—Fisheye, PTZ Preset Positions and PTZ on Event.

    4. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

View Video from Cameras in the Management Application

You can view live video from single cameras directly in the Management Application:

1. In the Management Application's navigation pane, expand *Advanced Configuration*, and expand *Cameras and Storage Information*.

2. Select the required camera to view live video from that camera. Above the live video, you will find a summary of the most important properties for the selected camera. Below the live video, you will find information about the camera's resolution and average image file size. For cameras using MPEG or H.264, you will also see the bit rate in Mbit/second.

IMPORTANT: Viewing of live video in the Management Application may, under certain circumstances, affect any simultaneous recording from the camera in question. The following three scenarios are important to consider:

1) Some cameras supporting multistreaming may have their frame rate reduced by half or respond with other negative effects when a second stream is opened.

2) If a camera delivers live video in very high quality, the de-coding of images may increase the load on the Recording Server service. This may, in turn, affect ongoing recordings negatively.

3) Cameras that do not support multiple simultaneous video streams will not be able to connect to the surveillance server and the Management Application at the same time; therefore it is recommended to stop the Recording Server service when configuring such devices for motion detection and PTZ.

Configure When Cameras Should Do What

Use the scheduling feature to configure when:

- Cameras should be online (that is, transfer video to RC-P)
- Cameras should use speedup (i.e. use a higher than normal frame rate)
- You want to receive any e-mail notifications regarding cameras
- Archiving should take place

See Configure General Scheduling & Archiving and Configure Camera-specific Schedules.

Monitor Storage Space Usage

To view how much storage space you have used and how much space is free on your RC-P system, do the following:

1. In the Management Application's navigation pane, expand *Advanced Configuration*, and select *Cameras and Storage Information*.

2. View the *Storage Usage Summary* for the following information: which drives are available, what drives are used for, the size of each drive, as well as how much video data, other data, and free space there is in each drive.

Database Resizing

In case the recordings for a camera get bigger than expected, or the available drive space is suddenly reduced in another way, an advanced database resizing procedure will automatically take place:

If archives are present on the same drive as the camera's database, the oldest archive for all cameras archived on that drive will be moved to another drive (moving archives is only possible if you use dynamic archiving, with which you can archive to several different drives) or—if moving is not possible—deleted.

If no archives are present on the drive containing the camera's database, the size of all camera databases on the drive will be reduced by deleting a percentage of their oldest recordings, thus temporarily limiting the size of all databases

When the Recording Server service is restarted upon such database resizing, the original database sizes will be used. You should therefore make sure that the drive size problem is solved.

Should the database resizing procedure take place, you will be informed in log files, and (if set up) through an e-mail notification.

Disable or Delete Cameras

All cameras are enabled by default . This means video from the cameras can be transferred to RC-P—provided that the cameras are scheduled to be online.

To **disable** a camera:

1. In the Management Application's navigation pane, expand *Advanced Configuration*, expand *Cameras and Storage Information*, double-click the camera you want to disable, and clear the *Enabled* checkbox.

2. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

To **delete** a camera, you technically have to delete the hardware device. Deleting the hardware device will also delete any attached microphones. If you do not want this, consider disabling the camera instead.

Wizards

Configure Video & Recording Wizard

The Configure Video and Recording wizard helps you quickly configure your cameras' video and recording properties. The wizard is divided into a number of pages:

- Video Settings and Preview
- Online Schedule
- Live and Recording Settings (Motion-JPEG Cameras)
- Live and Recording Settings (MPEG Cameras)
- Drive Selection
- Recording and Archiving Settings

Adjust Motion Detection Wizard

The Adjust Motion Detection wizard helps you quickly configure your cameras' motion detection properties. The wizard is divided into two pages:

- Exclude Regions
- Motion Detection

Cameras that do not support multiple simultaneous video streams will not be able to connect to the surveillance server and the Management Application at the same time; therefore it is recommended to stop the Recording Server service when configuring such devices for motion detection and PTZ. See also View Video from Cameras in Management Application.

General Recording & Storage Properties

Recording & Archiving Paths

All properties on a white background are editable, properties on a light blue background cannot be edited. Note that all of the Recording and Archiving Paths properties can also be specified individually for each camera.

- ***Template*:** The template can help you configure similar properties quickly. For example: you have 50 cameras and you want to change the recording path, archiving path, and retention time for all of them. Instead of having to enter the same three pieces of information 50 times, you can simply enter them once in the template, and then apply the template to the 50 cameras with only two clicks.

- ***Apply Template*:** Lets you select which cameras you want to apply the template for. You then use one of the two *Set* buttons (see descriptions in the following) to actually apply the template.

- ***Camera Name*:** Name of the camera as it will appear in the Management Application as well as in clients. If required, you can overwrite the existing camera name with a new one. Camera names must be unique, and must not contain any of the following special characters: `< > & ' " \ / : * ? | [ ]`

- ***Shortcut*:** Camera shortcut may be used in certain access clients.

- ***Recording Path*:** Path to the folder in which the camera's database should be stored. Default is C:\VideoData. To browse for another folder, click the browse icon next to the required cell. You are only able to specify a path to a folder on a *local* drive. You cannot specify a path to a network drove. The reason for this limitation is that if you were using a network drive, it would not be possible to save recordings if the network drive became unavailable. If you change the recording path, and there are existing recordings at the old location, you will be asked whether you want to move the recordings to the new location (recommended), leave them at the old location, or delete them.

- ***Archiving Path*:** Only editable if not using dynamic paths for archiving. Path to the folder in which the camera's archived recordings should be stored. Default is C:\VideoData. To browse for another folder, click the browse icon next to the required cell. You can only specify a path to local drive. If you change the archiving path, and there are existing archived recordings at the old location, you will be asked whether you want to move the archived recordings to the new location (recommended), leave them at the old location, or delete them. Note that if moving archived recordings, RC-P will also archive what is currently in the camera's database; in case you wonder why the camera database is empty just after you have moved archived recordings, this is the reason.

- ***Retention Time*:** Total amount of time for which you want to keep recordings from the camera (that is recordings in the camera's database as well as any archived recordings). Default is 30 days.

- ***Camera*:** Click the ***Open*** button to configure detailed and/or camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for the selected camera.

- ***Select All*:** Click button to select all cameras in the *Apply Template* column.

- ***Clear All*:** Click button to clear all selections in the *Apply Template* column

- ***Set selected template value on selected cameras*:** Lets you apply one or more selected values from the template (rather than all values) to selected cameras.

- ***Set all template values on selected cameras*:** Lets you apply all values from the template to selected cameras.

Dynamic Path Selection

With dynamic archiving paths, you specify a number of different archiving paths, usually across several drives. If the path containing the RC-P database on one of the drives you have selected for archiving, RC-P will always try to archive to that drive first. If not, RC-P automatically archives to the archiving drive with the most available space at any time, provided there is not a camera database using that drive. Which drive that is may change during the archiving process, and archiving may therefore happen to several archiving drives during the same process. This fact will have no impact on how users find and view archived recordings.

Dynamic archiving paths are general for all your cameras; you cannot configure dynamic archiving paths for individual cameras.

All properties on a white background are editable, properties on a light blue background cannot be edited.

- ***Enable dynamic path selection archives*:** Enables the use of dynamic path selection, allowing you to select which paths you want to use. The list of selectable paths initially represents all drives on the server, both local and mapped drives. You can add further paths with the *New path* feature below the list.
- ***Use*:** Lets you select particular paths for use as dynamic archiving paths. Also lets you select a previously manually added path for removal (see description of *Remove* button in the following)
- ***Drive*:** Indicates which drive the path belongs on.
- ***Path*:** Path to use as dynamic archiving path.
- ***Drive Size*:** Total amount of space on the drive, that is free space as well as used space.
- ***Free Space*:** Amount of free space available on the drive in question.
- ***New path*:** Lets you specify a new path, and add it to the list using the *Add* button. Paths must be reachable by the surveillance system server, and you must specify the path using the UNC (Universal Naming Convention) format, example: *server**volume**directory*\. When the new path is added, you can select it for use as a dynamic archiving path.
- ***Add*:** Lets you add the path specified in the *New path* field to the list.
- ***Remove*:** Lets you remove a selected path—which has previously been manually added—from the list. You cannot remove any of the initially listed paths, not even when they are selected.

Video Recording

In RC-P, the term *recording* means *saving video and, if applicable, audio from a camera in the camera's database on the surveillance system server*. Video/audio is often saved only when there is a reason to do so, for example as long as motion is detected, when an event occurs and until another event occurs, or within a certain period of time.

All properties on a white background are editable, properties on a light blue background cannot be edited. Note that all of the Video Recording properties can also be specified individually for each camera.

- ***Template*:** The template can help you configure similar properties quickly. For example: you have 50 cameras and you want 10 seconds of pre-recording on all of them. Instead of having to enter the same piece of information 50 times, you can simply enter it once in the template, and then apply the template to the 50 cameras with only two clicks.
- ***Apply Template*:** Lets you select which cameras you want to apply the template for. You then use one of the two *Set* buttons (see descriptions in the following) to actually apply the template.
- ***Camera Name*:** Name of the camera as it will appear in the Management Application as well as in clients. If required, you can overwrite the existing camera name with a new one. Camera names must be unique, and must not contain any of the following special characters: `< > & ' " \ / : * ? | [ ]`
- ***Record on*:** Lets you select under which conditions video from the camera should be recorded:
  - ***Always*:** Record whenever the camera is enabled and scheduled to be online (the latter allows for time-based recording).
  - ***Never*:** Never record. Live video will be displayed, but—since no video is kept in the database—users will not be able to play back video from the camera.
  - ***Motion Detection*:** Select this to record video in which motion is detected. Unless post-recording (see the following) is used, recording will stop immediately after the last motion is detected.
  - ***Event*:** Select this to record video when an event occurs and until another event occurs. Use of recording on event requires that events have been defined, and that you select start and stop events in the neighboring columns.

  - ***Motion Detection & Event*:** Select this to record video in which motion is detected, or when an event occurs and until another event occurs. Remember to select start and stop events in the neighboring columns.

- ***Start Event*:** Use when recording on Event or Motion Detection & Event. Select required start event. Recording will begin when the start event occurs (or earlier if using pre-recording; see the following).

- ***Stop Event*:** Select required stop event. Recording will end when the stop event occurs (or later if using post-recording; see the following).

- ***Pre-recording*:** You can store recordings from periods preceding detected motion and/or start events. Select check box to enable this feature. Remember to specify required number of seconds in the neighboring column.

  How does pre- and post-recording work? RC-P receives video in a continuous stream from the camera whenever the camera is enabled and scheduled to be online. This is what lets you view live video, but it also means that RC-P can easily store received video for a number of seconds in its memory (a.k.a. buffering). If it turns out that the buffered video is needed for pre- or post-recording, it is automatically appended to the recording. If not, it is simply discarded.

- ***Seconds [of pre-recording]*:** Specify the number of seconds for which you want to record video from before recording start conditions (that is motion or start event) are met. Usually, only some seconds of pre-recording is required, but you can specify up to 65535 seconds of pre-recording, corresponding to 18 hours, 12 minutes and 15 seconds. However, if specifying a very long pre-recording time, you can potentially run into a scenario where your pre-recording time spans scheduled or unscheduled archiving times. That can be problematic since pre-recording does not work well during archiving.

- ***Post-recording*:** You can store recordings from periods following detected motion and/or stop events. Select check box to enable this feature. Remember to specify required number of seconds in the neighboring column.

- ***Seconds [of post-recording]*:** Specify the number of seconds for which you want to record video from after recording stop conditions (that is motion or stop event) are met. Usually, only some seconds of post-recording is required, but you can specify up to 65535 seconds of post-recording, corresponding to 18 hours, 12 minutes and 15 seconds. However, if specifying a very long post-recording time, you can potentially run into a scenario where your post-recording time spans scheduled or unscheduled archiving times. That can be problematic since post-recording does not work well during archiving.

- ***Camera:*** Click the ***Open*** button to configure detailed and/or camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for the selected camera.

- ***Select All*:** Click button to select all cameras in the *Apply Template* column.

- ***Clear All*:** Click button to clear all selections in the *Apply Template* column

- ***Set selected template value on selected cameras*:** Lets you apply only a selected value from the template to selected cameras.

- ***Set all template values on selected cameras*:** Lets you apply all values from the template to selected cameras.

Manual Recording

When manual recording is enabled, Ocularis Client users with the necessary rights can manually start recording if they see something of interest while viewing live video from a camera which is not already recording.

If enabled, manual recording can thus take place even if recording for individual cameras is set to *Never* or *Conditionally*.

When started from the Ocularis Client, such user-driven recording will always take place for a fixed time, for example for five minutes.

- ***Enable manual recording*:** Select check box to enable manual recording and specify further details.

- ***Default duration of manual recording*:** Period of time (in seconds) during which user-driven recording will take place. Default duration is 300 seconds, corresponding to five minutes.

- ***Maximum duration of manual recording*:** Maximum allowed period of time for user-driven recording. This maximum is not relevant in connection with manual recording started from the Ocularis Client, since such manual recording will always take place for a fixed time. In some installations it is, however, also possible to

combine manual recording with third-party applications if integrating these with RC-P through an API or similar, and in such cases specifying a maximum duration may be relevant. If you are simply using manual recording in connection with the Ocularis Client, disregard this property.

Frame Rate - MJPEG

All properties on a white background are editable, properties on a light blue background cannot be edited. Note that all of the Frame Rate - MJPEG properties can also be specified individually for each camera using MJPEG.

- ### Template and Common Properties

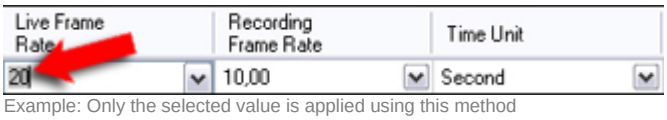
  - ***Template*:** The template can help you configure similar properties quickly. For example: you have 50 cameras and you want a particular frame rate on all of them. Instead of having to enter the same piece of information 50 times, you can simply enter it once in the template, and then apply the template to the 50 cameras with only two clicks.

  - ***Apply Template*:** Lets you select which cameras you want to apply the template for. You then use one of the two *Set* buttons (see descriptions in the following) to actually apply the template.

  - ***Select All*:** Click button to select all cameras in the *Apply Template* column.

  - ***Clear All*:** Click button to clear all selections in the *Apply Template* column

  - ***Set selected template value on selected cameras*:** Lets you apply only a selected value from the template to selected cameras.



Example: Only the selected value is applied using this method

  - ***Set all template values on selected cameras*:** Lets you apply all values from the template to selected cameras.

  - ***Camera Name*:** Name of the camera as it will appear in the Management Application as well as in clients. If required, you can overwrite the existing camera name with a new one. Camera names must be unique, and must not contain any of the following special characters: < > & ' " \ / : * ? | [ ]

- ### Regular Frame Rate Properties

  - ***Live frame rate*:** Required average frame rate for live video from the camera. Select number of frames, then select required interval (per second, minute or hour) in the *Frame Rate Time Base* column.

  - ***Recording frame rate*:** Required average frame rate for recorded video from the camera. Select number of frames, then select required interval (per second, minute or hour) in the *Frame Rate Time Base* column.

  - ***Frame Rate Time Base*:** Select required unit for live and recording frame rates (per second, minute, or hour).

  - ***Camera:*** Click the ***Open*** button to configure detailed and/or camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for the selected camera.

- ### Speedup Frame Rate Properties

  - ***Enable Speedup*:** The speedup feature lets you use a higher than normal frame rate if motion is detected and/or an event occurs. When you enable speedup, further columns for specifying speedup details become available.

  - ***Live Frame Rate*:** Required average speedup frame rate for viewing live video from the camera. Select number of frames, then select required interval (per second, minute or hour) in the *Frame Rate Time Base* column. The frame rate must be higher than the live frame rate specified under normal mode.

- ***Recording frame rate*:** Required average speedup frame rate for viewing recorded video from the camera. Select number of frames, then select required interval (per second, minute or hour) in the *Frame Rate Time Base* column. The frame rate must be higher than the recording frame rate specified under normal mode.

- ***Frame Rate Time Base*:** Select required unit for live and recording speedup frame rates (per second, minute, or hour). Note that you can only select time bases that let you speed up frame rates. Example: If you have specified 15 frames per *second* in normal mode, you cannot specify 16 frames per *minute* or *hour* in speedup mode.

- ***Speedup on*:** Lets you select under which conditions to use speedup frame rates:

    - ***Motion Detection*:** Select this to speed up when motion is detected. Normal frame rates will be resumed immediately after the last motion is detected.

    - ***Event*:** Select this to speed up when an event occurs and until another event occurs. Use of speedup on event requires that events have been defined, and that you select start and stop events in the neighboring columns.

    - ***Motion Detection & Event*:** Select this to speed up when motion is detected, or when an event occurs and until another event occurs. Remember to select start and stop events in the neighboring columns.

    - ***Schedule only*:** Select this to speed up according to the camera's speedup schedule only.

- ***Start Event*:** Select required start event. The camera will begin using the speedup frame rates when the start event occurs.

- ***Stop Event*:** Select required start event. The camera will return to the normal frame rates when the stop event occurs.

- ***Camera:*** Click the ***Open*** button to configure detailed and/or camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for the selected camera.

Frame Rate - MPEG

All properties on a white background are editable, properties on a light blue background cannot be edited. Note that all of the Frame Rate - MPEG properties can also be specified individually for each camera using MPEG.

- ***Template*:** The template can help you configure similar properties quickly. For example: you have 50 cameras and you want a particular frame rate on all of them. Instead of having to enter the same piece of information 50 times, you can simply enter it once in the template, and then apply the template to the 50 cameras with only two clicks.

- ***Apply Template*:** Lets you select which cameras you want to apply the template for. You then use one of the two *Set* buttons (see descriptions in the following) to actually apply the template.

- ***Camera Name*:** Name of the camera as it will appear in the Management Application as well as in clients. If required, you can overwrite the existing camera name with a new one. Camera names must be unique, and must not contain any of the following special characters: < > & ' " \ / : * ? | [ ]

- ***Live FPS*:** Lets you select the camera's live frame rate per second (FPS).

- ***Record Keyframe Only*:** Keyframes stored at specified intervals record the entire view of the camera, whereas the following frames record only pixels that change; this helps greatly reduce the size of MPEG files. Select the check box if you only want to record keyframes. Note that you can specify exceptions in the neighboring column.

- ***Record All Frames on*:** Allows you to make exceptions if you have selected *Record Keyframes Only*:

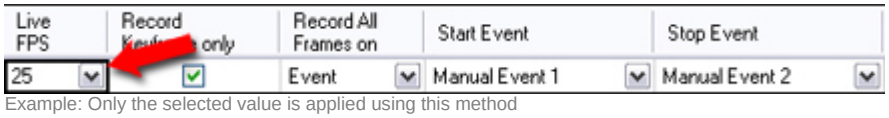
    - ***Motion Detection*:** Select this to record all frames when motion is detected. Two seconds after the last motion is detected, the camera will return to recording keyframes only.

    - ***Event*:** Select this to record all frames when an event occurs and until another event occurs. Requires that events have been defined, and that you select start and stop events in the neighboring columns.

Tip: If you have not yet defined any suitable events, you can quickly do it: Use the *Configure events* list, located in the bottom left corner of the window.

- ***Motion Detection & Event*:** Select this to record all frames when motion is detected, or when an event occurs and until another event occurs. Remember to select start and stop events in the neighboring columns.
- ***Schedule only*:** Select this to record all frames according to the camera's speedup schedule only.

- ***Start Event*:** Select required start event. The camera will begin recording all frames when the start event occurs.
- ***Stop Event*:** Select required start event. The camera will return to only recording keyframes when the stop event occurs.
- ***Camera:*** Click the ***Open*** button to configure detailed and/or camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for the selected camera.
- ***Select All*:** Click button to select all cameras in the *Apply Template* column.
- ***Clear All*:** Click button to clear all selections in the *Apply Template* column
- ***Set selected template value on selected cameras*:** Lets you apply only a selected value from the template to selected cameras.



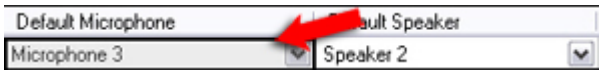
Example: Only the selected value is applied using this method

- ***Set all template values on selected cameras*:** Lets you apply all values from the template to selected cameras.

Audio Selection

With a default microphone and/or speaker selected for a camera, audio from the microphone will automatically be used when video from the camera is viewed. Note that all of the Audio Selection properties can also be specified individually for each camera.

- ***Template*:** The template can help you configure similar properties quickly. For instance: if you have 8 cameras and you want a particular default microphone for all of them. Instead of having to enter the same piece of information eight times, you can simply enter it once in the template, and then apply the template to the 8 cameras with only two clicks.
- ***Apply Template*:** Lets you select which cameras you want to apply the template for. You then use one of the two *Set* buttons (see descriptions in the following) to actually apply the template.
- ***Camera Name*:** Name of the camera as it will appear in the Management Application as well as in clients. If required, you can overwrite the existing camera name with a new one. Camera names must be unique, and must not contain any of the following special characters: < > & ' " \ / : * ? | [ ]
- ***Default Microphone*:** Select required default microphone.
- ***Camera:*** Click the ***Open*** button to configure detailed and/or camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for the selected camera.
- ***Select All*:** Click button to select all cameras in the *Apply Template* column.
- ***Clear All*:** Click button to clear all selections in the *Apply Template* column
- ***Set selected template value on selected cameras*:** Lets you apply only a selected value from the template to selected cameras.



Example: Only the selected value is applied using this method

- ***Set all template values on selected cameras*:** Lets you apply all values from the template to selected cameras.

Audio Recording

When you configure video and recording for specific cameras, you can determine whether audio should be recorded or not. Your choice will apply for all cameras on your RC-P system.

- ***Always*:** Always record audio on all applicable cameras.
- ***Never*:** Never record audio on any cameras. Note that even though audio is never recorded, it will still be possible to listen to live audio in the Ocularis Client.

If you record audio, it is important that you note the following:

- **Audio recording affects video storage capacity:** Audio is recorded to the associated camera's database. It is important to keep in mind that the database is likely to become full earlier if recording audio *and* video than if only recording video. The fact that the database becomes full is not in itself a problem since RC-P automatically archives data if the database becomes full. However, there is likely to be a greater need for archiving space if you record audio.
    - Example: If using MPEG4, each one-second video GOP (Group Of Pictures) will be stored in one record in the database. Each second of audio will also be stored in one record in the database. When this is the case, the database's video storage capacity will be halved, because half of the database's records will be used for storing audio. Consequently, the database will run full sooner, and automatic archiving will take place more often than if you were only recording video.
    - Example: If using MJPEG, audio is stored in one record for every JPEG for as long as the audio block size does not exceed the time between the JPEGs. The database's video storage capacity can thus in extreme cases be halved, because half of the database's records will be used for storing audio. If using very high frame rates, where there is less time between each JPEG, a smaller portion of the database will be used for storing audio records, and consequently a larger portion will be available for storing video. Anyway, the database will run full sooner, and automatic archiving will take place more often than if you were only recording video.

  Above examples are simplified, the exact available video storage capacity will also depend on GOP/JPEG and audio kilobyte size.

Storage Information

The storage usage summary information lets you view how much storage space you have used and free on your RC-P system:

- ***Drive*:** Letter representing the drive in question, for example C:.
- ***Path*:** Path to the storage area, for example C:\ or \\OurServer\OurFolder\OurSubfolder\.
- ***Usage*:** What the storage area is used for, for example recording or archiving.
- ***Drive Size*:** Total size of the drive.
- ***Video Data*:** Amount of video data on the drive.
- ***Other Data*:** Amount of other data on the drive.
- ***Free Space*:** Amount of unused space left on the drive.

Camera-Specific Properties

Camera

- ***Enabled*:** Cameras are by default enabled, meaning that provided they are scheduled to be online, they are able to transfer video to RC-P. If required, you can disable an individual camera, in which case no video/audio will be transferred from the camera source to RC-P.

- ***Camera name*:** Name of the camera as it will appear in the Management Application as well as in clients. If required, you can overwrite the existing camera name with a new one. Camera names must be unique, and must not contain any of the following special characters: < > & ' " \ / : * ? | [ ]

  Tip: Camera names can be very long if required: the upper limit is more than 2000 characters, although such long camera names are hardly ever needed.

- ***Camera shortcut number*:** Users of some clients can take advantage of keyboard shortcuts, some of which let the users toggle between viewing different cameras. Such shortcuts include numbers which are used to identify each camera.

Frame Rate

- ### If the Camera Uses the MJPEG Video Format

  With MJPEG, you can define frame rates for regular as well as speedup modes:

  Regular Frame Rate Mode:

  - ***Live frame rate*:** Frame rate for viewing live video from the camera. Select number of frames in the first field, and required interval (per second, minute or hour) in the second field.

  - ***Recording frame rate*:** Frame rate for viewing recorded video from the camera. Select number of frames in the first field, and required interval (per second, minute or hour) in the second field.

  Speedup Frame Rate Mode:

  - ***Enable speedup frame rate*:** The speedup feature lets you use a higher than normal frame rate if motion is detected and/or an event occurs. When you enable speedup, further fields for specifying speedup details become available.

  - ***Live frame rate*:** Speedup frame rate for viewing live video from the camera. Select number of frames in the first field, and required interval (per second, minute or hour) in the second field. The frame rate must be higher than the live frame rate specified under normal mode.

  - ***Recording frame rate*:** Speedup frame rate for viewing recorded video from the camera. Select number of frames in the first field, and required interval (per second, minute or hour) in the second field. The frame rate must be higher than the recording frame rate specified under normal mode.

  - ***On motion*:** Select this check box to use the speedup frame rates when motion is detected. The camera will return to the normal frame rates two seconds after the last motion is detected.

  - ***On event*:** Select this check box to use the speedup frame rates when an event occurs and until another event occurs. Use of speedup on event requires that events have been defined, and that you select start and stop events in the neighboring lists.

  - ***Start event*:** Select required start event. The camera will begin using the speedup frame rates when the start event occurs.

  - ***Stop event*:** Select required start event. The camera will return to the normal frame rates when the stop event occurs.

- ### If the Camera Uses the MPEG Video Format

  With MPEG, you can define frame rate as well as when to record keyframes or all frames:

  - ***Frame rate per second*:** Frame rate for viewing live and recorded video from the camera. Select number of frames per second.

  - ***Record keyframes only*:**Keyframes stored at specified intervals record the entire view of the camera, whereas the following frames record only pixels that change; this helps greatly reduce the size of MPEG files. Select the check box if you only want to record keyframes. Note that you can specify exceptions if motion is detected or events occur (see the following).

  - ***Record all frames on motion*:** Allows you to make exceptions if you have selected *record keyframes only*. Select this check box to record all frames when motion is detected. Two seconds after the last motion is detected, the camera will return to recording keyframes only.

  - ***Record all frames on event*:** Allows you to make exceptions if you have selected *record keyframes only*. Select this check box to record all frames when an event occurs and until another event occurs. Use of this feature requires that events have been defined, and that you select start and stop events in the neighboring lists.

  - ***Start event*:** Select required start event. The camera will begin recording all fames when the start event occurs.

  - ***Stop event*:** Select required start event. When the stop event occurs, the camera will return to recording keyframes only.

Video

When you configure video and recording for specific cameras, properties are to a large extent camera-specific. Since such properties vary from camera to camera, descriptions in the following are for guidance only.

If the selected camera is accessible, a live preview is displayed. Click the *Configure Video Properties* button to open a separate window with properties for the selected camera.

The video properties typically let you control bandwidth, brightness, compression, contrast, resolution, rotation, etc. by overwriting existing values of selecting new ones.

When adjusting video settings, you are—for most cameras—able to preview the effect of your settings in an image below the fields.

Video settings may feature an *Include Date and Time* setting. If set to *Yes*, date and time from the camera will be included in video. Note, however, that cameras are separate units which may have separate timing devices, power supplies, etc. Camera time and RC-P system time may therefore not correspond fully, and this may occasionally lead to confusion. As all frames are time-stamped by RC-P upon reception, and exact date and time information for each image is already known, it is recommended that the setting is set to *No*.

Audio

With a default microphone selected for a camera, audio from the microphone will automatically be used when video from the camera is viewed.

If a microphone is attached to the same hardware device as the camera, that microphone will be the camera's default microphone if you do not select otherwise.

- ***Default microphone*:** Select required microphone.

The ability to select a default microphone for the camera requires that at least one microphone has been attached to a hardware device on the surveillance system.

Recording Settings

In RC-P, the term *recording* means *saving video and, if applicable, audio from a camera in the camera's database on the surveillance system server*. Video/audio is often saved only when there is a reason to do so, for example as long as motion is detected, when an event occurs and until another event occurs, or within a certain period of time.

When you configure video and recording for specific cameras, recording properties include:

- ***Always*:** Record whenever the camera is enabled and scheduled to be online (the latter allows for time-based recording).
- ***Never*:** Never record. Live video will be displayed, but—since no video is kept in the database—users will not be able to play back video from the camera.
- ***Conditionally*:** Record when certain conditions are met. When you select this option, specify required conditions (see the following).
- ***On built-in motion detection*:** Select this check box to record video in which motion is detected. Unless post-recording (see the following) is used, recording will stop immediately after the last motion is detected.
- ***On event*:** Select this check box to record video when an event occurs and until another event occurs. Use of recording on event requires that events have been defined, and that you select start and stop events in the neighboring lists.
- ***Start event*:** Select required start event. Recording will begin when the start event occurs (or earlier if using pre-recording; see the following).
- ***Stop event*:** Select required start event. Recording will end when the stop event occurs (or later if using post-recording; see the following).

When the option *Conditionally* is selected, you can store recordings from periods preceding and following detected motion and/or specified events. Example: If you have defined that video should be stored when a door is opened, being able to see what happened immediately prior to the door being opened may also be important. For example, you may have specified that video should be stored conditionally on event, with a start event called Door Opened and a stop event called Door Closed. With three seconds of pre-recording, video will be recorded from three seconds before Door Opened occurs and until Door Closed occurs.

- ***Enable pre-recording*:** Available only when the option *Conditional* is selected. Specify the number of seconds for which you want to record video from before recording start conditions (that is motion or start event) are met.
- ***Enable post-recording*:** Available only when the option Conditional is selected. Specify the number of seconds for which you want to record video after recording stop conditions (that is motion end or stop event) are met.

How does pre- and post-recording work? RC-P receives video in a continuous stream from the camera whenever the camera is enabled and scheduled to be online. This is what lets you view live video, but it also means that RC-P can easily store received video for a number of seconds in its memory (a.k.a. buffering). If it turns out that the buffered video is needed for pre- or post-recording, it is automatically appended to the recording. If not, it is simply discarded.

Recording & Archiving Paths

- ***Recording path*:** Path to the folder in which the camera's database should be stored. Default is C:\VideoData. To browse for another folder, click the browse button next to the *Recording path* field. You are only able to specify a path to a folder on a *local* drive. If using a network drive, it would not be possible to save recordings if the network drive became unavailable.

  If you change the recording path, and there are existing recordings at the old location, you will be asked whether you want to move the recordings to the new location (recommended), leave them at the old location, or delete them.

- ***Delete Database*:** Click button to delete all recordings in the database for the camera. Archived recordings will not be affected.

  IMPORTANT: Use with caution; all recordings in the database for the camera will be permanently deleted. As a security measure, you will be asked to confirm the deletion.

- ***Archiving path*:** Only available if not using dynamic paths for archiving. Path to the folder in which the camera's archived recordings should be stored. Default is C:\VideoData\Archives. To browse for another folder, click the browse button next to the *Archiving path* field. You can only specify a path to local drive. If you change the archiving path, and there are existing archived recordings at the old location, you will be asked whether you want to move the archived recordings to the new location (recommended), leave them at the old location, or delete them. Note that if moving archived recordings, RC-P will also archive what is currently in the camera's

database; in case you wonder why the camera database is empty just after you have moved archived recordings, this is the reason.

- ***Delete Archives*:** Click button to delete all archived recordings for the camera. Recordings in the camera's regular database will not be affected. The ability to delete is available regardless of whether you use a single archiving path or dynamic archiving paths.

  IMPORTANT: Use with caution; all archived recordings for the camera will be permanently deleted. As a security measure, you will be asked to confirm the deletion.

- ***Retention time*:** Total amount of time for which you want to keep recordings from the camera (that is recordings in the camera's database as well as any archived recordings). Default is 30 days.

  Note that the retention time covers the **total** amount of time you want to keep recordings for; in earlier RC-P versions time limits were specified separately for the database and archives.

- ***Database repair action*:** Select which action to take if the database becomes corrupted:

  - *Repair, scan, delete if fails*: Default action. If the database becomes corrupted, two different repair methods will be attempted: a fast repair and a thorough repair. If both repair methods fail, the contents of the database will be deleted.
  - *Repair, delete if fails*: If the database becomes corrupted, a fast repair will be attempted. If the fast repair fails, the contents of the database will be deleted.
  - *Repair, archive if fails*: If the database becomes corrupted, a fast repair will be attempted. If the fast repair fails, the contents of the database will be archived.
  - *Delete (no repair)*: If the database becomes corrupted, the contents of the database will be deleted.
  - *Archive (no repair)*: If the database becomes corrupted, the contents of the database will be archived.

  No video can be recorded in a database while it is being repaired. For large installations, a repair may take several hours, especially if the *Repair, scan, delete if fails* action (which involves two different repair methods) is selected, and the first repair method (fast repair) fails.

  Tip: There are several things you can do to prevent that your databases become corrupt in the first place. See Protect Recording Databases from Corruption.

- ***Configure Dynamic Paths*:** With dynamic archiving paths, you specify a number of different archiving paths, usually across several drives. If the drive containing the camera's database is among the path you have selected for dynamic archiving, RC-P will always try to archive to that path first. If not, RC-P automatically archives to the archiving path with the most available space at any time, provided there is not a camera database using that drive. See also Dynamic Path Selection.

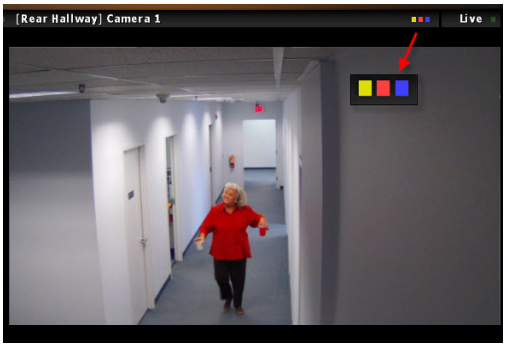
Event Notification

When you configure video and recording for specific cameras, properties include event notification:

- ### What Is an Event Notification?

  Event notification lets you inform Ocularis Client users that an event has occurred on the RC-P system. Event notification can be valuable for client users, as they will be able to quickly detect that an event has occurred, even though their focus was perhaps on something else the moment the event occurred.

In Ocularis Client, three differently colored indicators are available for each camera:



- The yellow event indicator. When event notification is used for a camera, the yellow indicator will light up when a relevant event has occurred.
- A red recording indicator; lights up when recording is taking place.
- A blue motion indicator; lights up when motion is occurring on the camera feed.

- ### How to Select Required Events

1. In the *Available events* list, select the required event. It is only possible to select one event at a time.
2. Click the >> button to copy the selected event to the *Selected Events* list.
3. Repeat for each required event.

If you later want to remove an event from the *Selected Events* list, simply select the event in question, and click the << button.

Output

When you configure video and recording for specific cameras, you are also able to associate a camera with particular hardware output, for example the sounding of a siren or the switching on of lights.

Associated output can then be activated automatically when motion is detected in video from the camera, or manually when Ocularis Client users with the necessary rights view live video from the camera.

1. In the *Available output* list, select the required output. It is only possible to select one output at a time.
2. Click the >> button to copy the selected output to:
   - the *On manual activation* list, in which case the output will be available for manual activation in the Ocularis Client.

     - and/or -

   - the *On motion detected* list, in which case the output will be activated when motion is detected in video from the camera.

   If required, the same output can appear on both lists.
3. Repeat for each required output.

If you later want to remove an output from the one of the lists, simply select the output in question, and click the << button.

Motion Detection & Exclude Regions

When you configure video and recording for specific cameras, adjusting motion detection is important since it may determine when video from the camera is recorded, when e-mail notifications are generated, when hardware output (such as lights or sirens) is activated, etc. Time spent on finding the best possible motion detection settings for each camera may help you later avoid unnecessary recordings, notifications, etc. Depending on the physical location of the camera, it may be a very good idea to test motion detection under different physical conditions (day/night, windy/calm weather, etc.).

Before you configure motion detection for a camera, it is highly recommended that you have configured the camera's video properties, such as compression, resolution, etc.

Cameras that do not support multiple simultaneous video streams will not be able to connect to the surveillance server and the Management Application at the same time; therefore it is recommended to stop the Recording Server service when configuring such devices for motion detection and PTZ. See also View Video from Cameras in Management Application.

- ## How to Configure Motion Detection Properties

1. Determine whether there are any areas which should be excluded from motion detection (for example if the camera covers an area where a tree is swaying in the wind or where cars regularly pass by in the background). If so, you can avoid detection of irrelevant motion by following the points below. If not, continue to step 2.

    - In the *Exclude regions* section in lower part of the window, select ***Enable***. The preview image is now divided into small sections by a grid. To define areas which should be excluded from motion detection, drag the mouse pointer over the required areas in the preview image while pressing the mouse button down. Left mouse button selects a grid section; right mouse button clears a grid section. Selected areas are highlighted in blue. Occasionally, you may also want to take advantage of further exclude regions features:

    - ***Show grid*****:** Lets you toggle the grid on and off. Toggling the grid off may provide a less obscured view of the preview image; selection of areas which should be excluded from motion detection takes place the same way as when the grid is visible.

    - ***Set All*****:** Lets you quickly select all grid sections in the preview image. This may be advantageous if you want to exclude motion detection in most areas of the image, in which case you can simply clear the few sections in which you do not want to exclude motion detection.

    - ***Clear All*****:** Lets you quickly clear all grid sections in the preview image.

    - ***Auto*****:** Makes RC-P automatically detect areas with insignificant changes in individual pixels which should not be regarded as motion, and automatically mark such areas for exclusion from motion detection. As the automatic detection is based on an analysis of one second of video, it may take a short while before you see the result.

      The automatic detection takes place according to the sensitivity setting specified in step 2. In order for the Auto feature to work as intended, it is therefore recommended that you go to step 2 and specify a sensitivity setting that matches your requirements before using the Auto feature.

2. Use the two sliders for configuring motion detection:

    - ***Sensitivity*****:** Determines how much each pixel must change before it is regarded as motion. With a high sensitivity, very little change in a pixel is required before it is regarded as motion. Areas in which motion is detected are highlighted in green in the preview image. Select a slider position in which only detections you consider motion are highlighted. As an alternative to using the slider, you may specify a value between 0 and 256 in the field next to the slider to control the sensitivity setting.

      Tip: If you find the concept of sensitivity difficult to grasp, try dragging the slider to its leftmost position: The more you drag the slider to the left, the more of the preview image becomes highlighted. This is because with a high sensitivity even the slightest change in a pixel will be regarded as motion.

    - ***Motion*****:** Determines how many pixels must change in the image before it is regarded as motion. The selected level is indicated by the black vertical line in the motion level indication bar below the preview image. The black vertical line serves as a threshold: When detected motion is above (that is to the right of) the selected sensitivity level, the bar changes color from green to red, indicating a positive detection. As an alternative to using the slider, you may specify a value between 0 and 10000 in the field next to the slider to control the motion setting.

3. Specify required ***Motion detection interval***, that is how often motion detection analysis should be carried out on video from the camera. The interval is measured in milliseconds; default is 240 milliseconds (that is close to once every quarter of a second). The interval is applied regardless of the camera's frame rate settings.

- ### Motion Detection and PTZ Cameras

  Motion detection generally works the same way for PTZ (Pan/Tilt/Zoom) cameras as it does for regular cameras. However:

  - It is not possible to configure motion detection separately for each of a PTZ camera's preset positions.

PTZ Preset Positions

PTZ-related properties are only available when you are dealing with a PTZ (Pan/Tilt/Zoom) camera. PTZ preset positions can be used for making the PTZ camera automatically go to a particular position when particular events occur. Preset positions also become selectable in clients, allowing users with required rights to move the PTZ camera between preset positions.

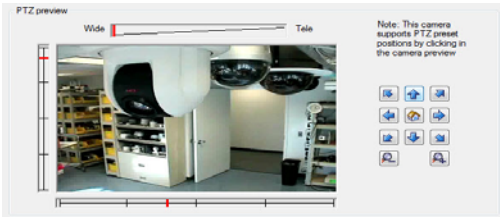
Names of preset positions must contain only the characters A-Z, a-z and the digits 0-9. If you import preset positions from cameras (see the following), verify that their names do not contain other characters; if they do, change the preset position names before importing them.

Restart services after having made changes to PTZ settings.

Cameras that do not support multiple simultaneous video streams will not be able to connect to the surveillance server and the Management Application at the same time; therefore it is recommended to stop the Recording Server service when configuring such devices for motion detection and PTZ. See also View Video from Cameras in Management Application.

- ***PTZ type*:** Your configuration options depend on the type of PTZ camera in question:
  - Type 1 (stored on server): You define preset positions by moving the camera using the controls in the upper half of the window, then storing each required position on the RC-P server. You can define up to 25 preset positions this way.
  - Type 2 (imported from camera): You import preset positions which have previously been defined and stored on the PTZ camera itself through the camera's own configuration interface. The number of allowed preset positions depends on the PTZ camera and driver used.
  - Type 3 (stored on camera): You define preset positions by moving the camera with the controls in the upper half of the window, then storing each required position in the camera's own memory. You are able to define up to 25 preset positions this way. If preset positions have already been defined for the camera, you can simply import them for use with RC-P.

  For PTZ types 1 and 3, you can move the PTZ camera to required positions:



  - By simply clicking the required position in the camera preview (if supported by the camera).
  - By using the sliders located near the camera preview to move the PTZ camera along each of its axes: the X-axis (for panning left/right), the Y-axis (for tilting up/down), and the Z-axis (for zooming in and out; to zoom in, move the slider towards *Tele;* to zoom out, move the slider towards *Wide*).
  - By using the navigation buttons:

Moves the PTZ camera up and to the left

Moves the PTZ camera up

Moves the PTZ camera up and to the right

Moves the PTZ camera to the left

Moves the PTZ camera to its home position (that is default position)

Moves the PTZ camera to the right

Moves the PTZ camera down and to the left

Moves the PTZ camera down

Moves the PTZ camera down and to the right

Zooms out (one zoom level per click)

Zooms in (one zoom level per click)

- ***Import / Refresh*:** Only available when you have selected PTZ type 2 or 3. Lets you import already defined preset positions from the camera's memory for use with RC-P. If you have already imported preset positions this way, and preset positions have since then been added or changed on the camera, you can use this button to refresh the imported preset positions.

- ***Add New*:** Only available when you have selected PTZ type 1. When you have move the camera to a required position using the controls in the upper half of the window, type a name for the position in the blank field, then click the button to add the position to the list of defined preset positions.

  Remember that names of preset positions must contain only the characters A-Z, a-z and the digits 0-9.

- ***Set New Position*:** Only available when you have selected PTZ type 1 or 3. Lets you change an already defined preset position. In the list, select the preset position you want to change. Then move the camera to the new required position using the controls in the upper half of the window. Then click the button to overwrite the old position with the new one.

- ***Delete*:** Only available when you have selected PTZ type 1 or 3. Lets you delete an already defined preset. In the list, select the preset position you want to delete, then click the button.

  Before you delete a preset position, make sure it is not used in PTZ patrolling or PTZ on event. Since the preset positions are stored on the camera, you can bring a deleted preset position back into RC-P by clicking the *Import / refresh* button. If you bring back a preset position this way, and the preset position is to be used in PTZ patrolling or PTZ on event, you must manually configure PTZ patrolling and/or PTZ on event to use the preset position again.

- ***Test*:** Lets you try out a preset position. In the list, select the preset position you want to test, then click the Test button to view the camera move to the selected position.

- ***and* :** Lets you move a preset position selected in the list up and down respectively. The selected preset position is moved one step per click. By moving preset positions up or down, you can control the sequence in which preset positions are presented in clients.

PTZ on Event

PTZ-related properties are only available when you are dealing with a PTZ (Pan/Tilt/Zoom) camera. When a PTZ camera supports preset positions, it is possible to make the PTZ camera automatically go to a particular preset position when a particular event occurs.

When associating events with preset positions on a PTZ camera, you are able to select between **all** events defined on your RC-P system; you are not limited to selecting events defined on a particular hardware device.

1. In the *Events* list in the left side of the window, select the required event.
2. In the *PTZ Preset Position* list in the right side of the window, select the required preset position.

For this purpose, you can only use an event once per PTZ camera. However, different events can be used for making the PTZ camera go to the same preset position. Example:

- Event 1 makes the PTZ camera go to preset position A
- Event 2 makes the PTZ camera go to preset position B
- Event 3 makes the PTZ camera go to preset position A

If you later want to end the association between a particular event and a particular preset position, simply clear the field containing the event.

Restart services after having made changes to PTZ settings.

Cameras that do not support multiple simultaneous video streams will not be able to connect to the surveillance server and the Management Application at the same time; therefore it is recommended to stop the Recording Server service when configuring such devices for motion detection and PTZ. See also View Video from Cameras in Management Application.

Events, Input & Output

Overview of Events, Input & Output

Hardware input, such as door sensors, etc. can be attached to input ports on hardware devices. Input from such external hardware input units can be used for generating events in RC-P.

Events of various types (see the following for details) can be used for automatically triggering actions in RC-P. Examples of actions: starting or stopping recording on cameras, switching to a particular video frame rate, triggering e-mail notifications, making PTZ cameras move to specific preset positions, etc. Events can also be used for activating hardware output.

Hardware output units can be attached to output ports on many hardware devices, allowing you to activate lights, sirens, etc. from RC-P. Such hardware output can be activated automatically by events, or manually from clients.

- ### Event Types

  - **Hardware input events:** Events based on input from hardware input units attached to hardware devices are called hardware input events.

    Some hardware devices have their own capabilities for detecting motion, for detecting moving and/or static objects, etc. (configured in the hardware devices' own software; typically by accessing a browser-based configuration interface on the hardware device's IP address). When this is the case, RC-P considers such detections as input from the hardware, and you can use such detections as input events as well.

    Lastly, hardware input events can be based on RC-P detecting motion in video from a camera, based on RC-P's motion detection settings. This type of hardware input events is also called system motion detection events or VMD(Video Motion Detection)events. In earlier RC-P versions, VMD events were an event type of their own; now they are simply considered a type of hardware input event.

  - **Manual events:** Events may be generated manually by users selecting them in their clients. These events are called manual events.

  - **Timer events:** Timer events are separate events, triggered by the hardware input event or manual event under which they are defined. Timer events occur a specified number of seconds or minutes after the event under which they are defined has occurred. Timer events may be used for a wide variety of purposes, typically for stopping previously triggered actions. Examples:

    - A camera starts recording based on a hardware input event, for example when a door is opened; a timer event stops the recording after 15 seconds
    - Lights are switched on and a camera starts recording based on a manual event; a timer event stops the recording after one minute, and another timer event switches the lights off after two minutes

  - **VMD events; where are they?** In previous versions of RC-P, an event type called VMD events existed. VMD (Video Motion Detection) events were based on the RC-P system detecting motion in the video stream from a camera. This is still possible, but now you configure such events as hardware input events.

- ### Things to Be Aware of

  Before you specify use of hardware input and hardware output units on a hardware device, verify that sensor operation is recognized by the hardware device. Most hardware devices are capable of showing this in their configuration interfaces, or via CGI script commands. Also check the RC-P release notes to verify that input and output controlled operations are supported for the hardware device and firmware used.

- ### Moving on

  You do not have to configure hardware input units separately, any hardware input units connected to hardware devices are automatically detected when you add the hardware devices to RC-P. The same goes for hardware output, but hardware output does require some simple configuration in RC-P.

Before configuring events of any type, **configure general event handling**, such as which ports RC-P should use for event data. Normally, you can just use the default values, but it is a good idea to verify that your organization is not already using the ports for other purposes. See Configure General Event Handling.

When you are ready to **configure events**, see Add a Hardware Input Event and Add a Manual Event. If you want to use timer events with your other events, see Add a Timer Event.

If you want to **configure hardware output** and **automatically trigger output when events occur**, so that, for example, lights are switched on when a door is opened or when motion is detected in video, see Add a Hardware Output and Configure Hardware Output on Event.

Configure General Event Handling

Before configuring events of any type, configure general event handling, such as which ports RC-P should use for event data. Normally, you can just use the default values, but it is a good idea to verify that your organization is not already using the ports for other purposes.

1. In the Management Application's navigation pane, expand *Advanced Configuration*, right-click *Events and Output*, and select *Properties.*
2. Specify required properties. When ready, click *OK*.
3. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

Add a Hardware Input Event

With hardware input events, you can turn input received from input units attached to hardware devices into events in RC-P.

Before you specify input for a hardware device, verify that sensor operation is recognized by the hardware device. Most hardware devices are capable of showing this in their configuration interfaces, or via CGI script commands. Also check the release notes to verify that input-controlled operation is supported for the hardware device and firmware used.

To add and/or configure a hardware input event, do the following:

1. In the Management Application's navigation pane, expand *Advanced Configuration,* then expand *Events and Output.* Right-click *Hardware Input Events* and select *Enable New Input Event*.
2. In the *Hardware Input Event Properties* window's list of hardware devices, expand the required hardware device to see a list of pre-defined hardware input.
3. Select the required types of input to use them as events. The types of input often vary from camera to camera. If motion detection is enabled in RC-P for the camera in question, note the input type *System Motion Detection*, which lets you turn detected motion in the camera's video stream into an event. In earlier RC-P versions, this was known as a VMD event.

   Note that some types of input are mutually exclusive. When you select one type of input, you may therefore note that other types of input become unavailable for selection.
4. For each selected type of input, select required properties. When ready, click *OK*, or click the *Add button* to add a timer event to the event you have just created.
5. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

Add a Manual Event

With manual events, your users with required rights can trigger events manually from their clients. Manual events can be global (shared by all cameras) or tied to a particular camera (only available when the camera is selected). You can use manual events for a wide variety of purposes, for example:

- As start and stop events for use when scheduling cameras' online periods. For example, you can make a camera start or stop transferring video to the surveillance system based on a manual event.
- As start and stop events for controlling other camera settings. For example, you can make a camera use a higher frame rate based on a manual event or you can use a manual event for triggering PTZ on event.
- For triggering output. Particular output can be associated with manual events.
- For triggering event-based e-mail notifications.
- In combinations. For example, a manual event could make a camera start transferring video to the surveillance system while an output is triggered and an e-mail notification is sent to relevant people.

To add a manual event, do the following:

1. In the Management Application's navigation pane, expand *Advanced Configuration,* then expand *Events and Output.* Right-click *Manual Events* and select *Add New Manual Event*
2. In the list in the left side of the *Manual Event Properties*, select global or a camera as required.
3. Click the *add* button and specify required properties. When ready, click *OK*, or click the *Add* button again to add a timer event to the event you have just created.
4. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

Add a Timer Event

Timer events are separate events, triggered by the hardware input event or manual event under which they are defined. Timer events occur a specified number of seconds or minutes after the event under which they are defined has occurred. Timer events may be used for a wide variety of purposes, typically for stopping previously triggered actions. Examples:

- A camera starts recording based on a hardware input event, for example when a door is opened; a timer event stops the recording after 15 seconds
- Lights are switched on and a camera starts recording based on a manual event; a timer event stops the recording after one minute, and another timer event switches the lights off after two minutes

To add a timer event, select any event you have previously configured, click the *Add* button, and specify required properties. When ready, click *OK*, and save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

Add a Hardware Output

With hardware output, you can add external output units, such as lights, sirens, door openers, etc., to your RC-P system. Once added, output can be activated automatically by events or detected motion, or manually by client users.

Before you specify output, verify that sensor operation is recognized by the hardware device with which you are going to use the output. Most hardware devices are capable of showing this in their configuration interfaces, or via CGI script commands. Also check the release notes to verify that output-controlled operation is supported for the hardware device and firmware used.

To add a hardware output event, do the following:

1. In the Management Application's navigation pane, expand *Advanced Configuration,* then expand *Events and Output.* Right-click *Hardware Output* and select *Add New Output*.
2. In the *Hardware Output Properties* window's list of hardware devices, select the required hardware device, and click the *Add* button below the list.
3. Specify required properties.
4. Click *OK*.
5. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

For information about how to configure automatic activation of hardware output when events occur, see Configure Hardware Output on Event.

You configure output for manual activation in clients as well as for automatic activation on detected motion individually for each camera.

Configure Hardware Output on Event

Once you have added hardware output, such as lights, sirens, door openers, etc., you can associate the hardware output with events. This way, particular hardware output can be activated automatically when events occur. Example: When a door is opened (hardware input event), lights are switched on (hardware output).

When making the associations, you can select between **all** output and events defined on your RC-P server; you are not limited to selecting output or events defined on particular hardware devices.

1. In the Management Application's navigation pane, expand *Advanced Configuration,* then expand *Events and Output.* Right-click *Output Control on Event* and select *Properties*.
2. In the *Event* column, select the required event.
3. In the *Output* column, select the hardware output you want to be activated by the event.
4. Click *OK*.
5. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

You can use a single event for activating more than one output.

You cannot delete associations, but you can change your selections or select *None* in both columns as required.

General Event Properties

Ports & Polling

The *General Event Properties* window lets you specify network settings to be used in connection with event handling.

- ***Alert port*:** Lets you specify port number to use for handling events. Default port is port 1234.
- ***SMTP event port*:** Lets you specify port number to use for sending event information from hardware devices to RC-P via SMTP. Default port is port 25.
- ***FTP event port*:** Lets you specify port number to use for sending event information from hardware devices to RC-P via FTP. Default port is port 21.
- ***Polling interval [1/10] second*:** For a small number of hardware devices, primarily dedicated input/output devices, it is necessary for RC-P to regularly check the state of the hardware devices' input ports in order to detect input. Such state checking at regular intervals is called polling. You can specify (in tenths of a second) the interval between state checks. Default value is 10 tenths of a second (that is one second). For dedicated input/output devices, it is highly recommended that the polling frequency is set to the lowest possible value (one tenth of a second between state checks). For information about which hardware devices require polling, see the release note.

Event- & Output-Specific Properties

Hardware Input Event

When adding hardware input events, some properties depend on the selected type of input:

- ***Enable*:** Select check box to use selected type of input as an event in RC-P, and specify further properties.
- ***Event name*:** Specify a name for the event. Hardware input event names must be unique, and must not contain the following characters: < > & ' " \ / : * ? | [ ]

  Some cameras only support event names of a certain length and/or with a certain structure. Refer to the camera's documentation for exact details.
- ***Images from camera*:** Only relevant if using pre- and post-alarm images, a feature available for selected cameras only; it enables sending of images from immediately before an event took place from the camera to the surveillance system via e-mail. Pre- and post-alarm images should not be confused with RC-P's own pre- and post-recording feature. Lets you select which camera you want to receive pre- and/or post-alarm images from.
- ***Number of pre-alarm images*:** Only relevant if using pre-alarm images, a feature available for selected cameras only. Specify required number of pre-alarm images. Allowed number may differ from camera to camera; allowed range is displayed to the right of the field.
- ***Frames per second*:** Only relevant if using pre-alarm images, a feature available for selected cameras only. Specify required frame rate. Used in combination with the *Number of pre-alarm images* field, this field indirectly allows you to control how long before the event you want to receive pre-alarm images from.
- ***Send e-mail if this event occurs*:** Only available if e-mail notification is enabled. Select if RC-P should automatically send an e-mail when the event occurs. Recipients are defined as part of the e-mail notification configuration. When using e-mail notifications, also keep in mind individual cameras' scheduling.
- ***Attach image from camera*:** Only available if e-mail notification is enabled. Select to include an image—recorded at the time the event is triggered—in the e-mail notification, then select the required camera in the list next to the check box.
- ***Delete*:** Lets you delete a selected timer event.
- ***Add*:** When a specific hardware input event is selected, clicking *Add* will add a timer event to the selected hardware input event.

Manual Event

- ***[List of defined global events and cameras]*:** Contains a *Global* node and a list of all defined cameras. You can configure as many manual events as required, no matter whether they are global or camera-specific. A + sign next to the *Global* node indicates that one or more global manual events have already been configured. A + sign next to a camera indicates that one or more manual events have already been configured for that camera.
- ***Event name*:** Specify a name for the event; this is the name that client users will see. Manual event names must be unique, and must not contain the following characters: < > & ' " \ / : * ? | [ ]

  Some cameras only support event names of a certain length and/or with a certain structure. Refer to the camera's documentation for exact details.
- ***Send e-mail if this event occurs*:** Only available if e-mail notification is enabled. Select if RC-P should automatically send an e-mail when the event occurs. Recipients are defined as part of the e-mail notification configuration. When using e-mail notifications, also keep in mind individual cameras' scheduling.
- ***Attach image from camera*:** Only available if e-mail notification is enabled. Select to include an image—recorded at the time the event is triggered—in the e-mail notification, then select the required camera in the list next to the check box.

- ***Delete*:** Lets you delete a selected event.

- ***Add*:** Lets you add a new event. When *Global* or a specific camera is selected, clicking *Add* will add a new manual event. When a specific manual event is selected, clicking *Add* will add a timer event to the selected manual event.

Timer Event

- ***Timer event name*:** Specify a name for the event. Timer event names must be unique, and must not contain the following characters: < > & ' " \ / : * ? | [ ]

  Some cameras only support event names of a certain length and/or with a certain structure. Refer to the camera's documentation for exact details.

- ***Timer event occurs after*:** Lets you specify the amount of time that should pass between the main event occurring and the timer event (in seconds or minutes).

Hardware Output

- ***Output name*:** Specify a name for the event. If you are going to make the hardware output available for manual activation in clients, this is the name that client users will see. Hardware output names must be unique, and must not contain the following characters: < > & ' " \ / : * ? | [ ]

  Some hardware devices only support hardware output names of a certain length and/or with a certain structure. Refer to the hardware device's documentation for exact details.

- ***Output connected to*:** Lets you select which of the hardware device's output ports the output is connected to. Many hardware devices only have a single output port; in that case simply select *Output 1*.

- ***Keep output for*:** Lets you specify the amount of time for which the output should be applied. Specify the required amount of time in either 1/10 seconds or seconds.

  Some hardware devices are only able to apply output for a relatively short time, for example for up to five seconds. Refer to the documentation for the hardware device in question for exact information.

Hardware Devices

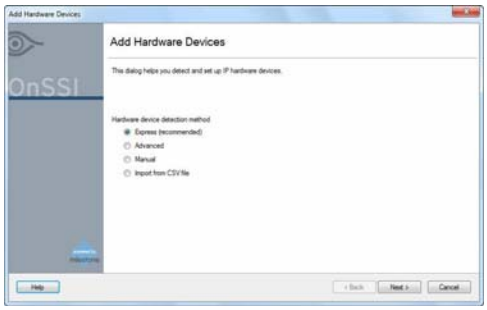
Add Hardware Devices

You add cameras and other hardware devices, such as video encoders, to your RC-P system through the Add Hardware Devices... wizard. If microphones are attached to a hardware device, they are automatically added as well.

You are allowed to use up to 25 cameras. Note that, if required, it is possible to *add* more cameras than you are allowed to use. If using video encoder devices on your system, keep in mind that many video encoder devices have more than one camera connected to them. For example, a fully used four-port video encoder will count as four cameras.

Before you begin using the wizard, it is highly recommended that you import your Device License Key file into RC-P. Importing the file is quick and easy, and it will free you from having to specify license keys manually for each hardware device later.

The wizard offers you four different ways of adding cameras:



- **Express (recommended):** Quickly scans your network for devices, and helps you quickly add them to your system. This method is quick and easy since it only scans for devices supporting device discovery, and only on the part of your network (subnet) where the RC-P server itself is located. Device discovery is a method with which hardware devices make information about themselves available on the network. Based on such information, RC-P can recognize relevant hardware devices on your network, and thus include, for example, cameras, but not printers, in the scan. To use the Express method, your RC-P server and your cameras must be on the same layer 2 network, that is a network where all servers, cameras, etc. can communicate without the need for a router. See Add Hardware Devices Wizard - Express.

- **Advanced:** Scans your network for hardware devices based on your specifications regarding required IP ranges, discovery methods, drivers, and device user names and passwords. See Add Hardware Devices Wizard - Advanced.

- **Manual:** Lets you specify details about each hardware device separately. A good choice if you only want to add a few hardware devices, and you know their IP addresses, required user names and passwords, etc. See Add Hardware Devices Wizard - Manual.

- **Import from CSV file:** Lets you import data about cameras as comma-separated values from a file; an effective method if setting up several similar systems. See Add Hardware Devices Wizard - Import from CSV File.

Configure Hardware Devices

Once you have added hardware devices, you can specify/edit device-specific properties, such as the IP address, which video channels to use, which COM ports to use for controlling attached PTZ (Pan/Tilt/Zoom) cameras, whether to use fisheye technology, etc.

1. In the Management Application's navigation pane, expand *Advanced Configuration*, expand *Hardware Devices*, right-click the required hardware device, and select *Properties*.

2. Specify Name & Video Channels, Network, Device Type & License, PTZ Device, and Fisheye properties as required.

3. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

Use Dedicated Input/Output Devices

It is possible to add a number of dedicated input/output (I/O) hardware devices to RC-P (see Add Hardware Devices). For information about which I/O hardware devices are supported, see the release notes.

When such I/O hardware devices are added, input on them can be used for generating events in RC-P, and events in RC-P can be used for activating output on the I/O hardware devices. This means that I/O hardware devices can be used in your events-based system setup in the same way as a camera.

When using some I/O hardware devices it is necessary for the surveillance system to regularly check the state of the hardware devices' input ports in order to detect whether input has been received. Such state checking at regular intervals is called *polling*. The interval between state checks, called a *polling frequency*, is specified as part of RC-P's general ports & polling properties. For such I/O hardware devices, the polling frequency should be set to the lowest possible value (one tenth of a second between state checks). For information about which I/O hardware devices require polling, see the release notes.

Replace Hardware Devices

If required, you can replace a hardware device—which you have previously added to and configured on your surveillance system—with a new one. This can typically be relevant if you replace a physical camera on your network.

The Replace Hardware Device wizard helps you through the entire replacement process on the surveillance system server, including:

- Detecting the new hardware device
- Specifying license for the new hardware device
- Deciding what to do with existing recordings from the old hardware device

You access the Replace Hardware Device wizard from the Management Application's navigation pane: Expand *Advanced Configuration*, expand *Hardware Devices*, right-click the hardware device you want to replace, and select *Replace Hardware Device*.

You can access also the wizard when dealing with a hardware device's Network, Device Type & License properties.

Delete Hardware Devices

IMPORTANT: Deleting a hardware device will not only delete all cameras and microphones attached to the hardware device. It will also delete any recordings from cameras on the hardware device.

1. In the Management Application's navigation pane, expand *Advanced Configuration*, expand *Hardware Devices*, right-click the hardware device you want to delete, and select *Delete Hardware device*.
2. Confirm that you want to delete the hardware device and all its recordings.
3. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.
4. Restart the Recording Server service.

If you find that deleting a hardware device is not the right thing to do, consider disabling the individual cameras or microphones connected to the hardware device instead:

1. In the Management Application's navigation pane, expand *Advanced Configuration*, expand *Hardware Devices*, and expand the hardware device in question.
2. Right-click the camera, microphone or speaker you want to disable, and select *Disable*.
3. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.
4. Restart the Recording Server service.

Add Hardware Devices Wizard

Express Method

The Express option scans your network for relevant hardware devices, and helps you quickly add them to your system. With the Express option, the wizard only scans for hardware devices supporting device discovery, and only on the part of your network (subnet) where the RC-P server itself is located.

What is device discovery? Device discovery is a method with which hardware devices make information about themselves available on the network. Based on such information, RC-P can quickly recognize relevant hardware devices, such as cameras and video encoders, and include them in the scan.

To use the Express method, **your RC-P server and your cameras must be on the same layer 2 network**; that is a network where all servers, cameras, etc. can communicate without the need for a router. The reason for this is that device discovery relies on direct communication between the RC-P server and the cameras. If you know that routers are used on your network, use the advanced or manual method instead.

If you are asked for Device License Keys (DLKs) when starting the wizard, see Import DLKs (Device License Keys).

When using the Express option, the wizard is divided into a number of pages:

- Hardware Detection and Verification
- Missing DLKs (if Applicable)
- Overview and Names

Advanced Method

The Advanced option scans your network for relevant hardware devices based on your specifications regarding required IP ranges, discovery methods, drivers, and device user names and passwords. If you are asked for Device License Keys (DLKs) when starting the wizard, see Import DLKs (Device License Keys).

When using the Advanced option, the wizard is divided into a number of pages:

- Device Discovery, IP Ranges, Drivers and Authentication
- Detected and Verified Hardware Devices
- Missing DLKs (if Applicable)
- Overview and Names

Manual Method

The Manual option lets you specify details about each hardware device separately. A good choice if you only want to add a few hardware devices, and you know their IP addresses, required user names and passwords, etc.

If you are asked for Device License Keys (DLKs) when starting the wizard, see Import DLKs (Device License Keys).

When using the Manual option, the wizard is divided into a number of pages:

- Hardware Device Information, Driver Selection and Verification
- Missing DLKs (if Applicable)
- Overview and Names

Import from CSV File Method

This option lets you import data about hardware devices and cameras as comma-separated values (CSV) from a file; a highly effective method if setting up several similar systems.

First select whether cameras and the RC-P server is online (that is having working network connections) or offline.

Then point to the CSV file, and click *Next*.

- ## CSV File Format and Requirements

  The CSV file must have a header line (defining each value on the subsequent lines), and subsequent lines must each contain information about one hardware device only. A minimum of information is always required for each hardware device, but note that the minimum required information is different depending on whether your server and cameras are online or offline.

  ### Cameras and Server Are Online

  If cameras and server are **online**, required information is:

  - ***HardwareAddress***
    IP address of the hardware device. Required format: IPv4 or IPv6.
  - ***HardwarePort***
    Port to use for HTTP communication with the hardware device. Default is port 80.
  - ***HardwarePassword***
    Password for the hardware device's administrator account. Most organizations use their own passwords rather than device manufacturers' passwords.

  ### Camera and Server Are Offline

  If cameras and server are **offline**, required information is:

  - ***HardwareAddress***
    IP address of the hardware device. Required format: IPv4 or IPv6.
  - ***HardwareMacAddress***
    MAC address of the hardware device. Examples of valid MAC address formats: 0011D81187A9, 0011d81187a9, 00:11:D8:11:87:A9, 00-11-D8-11-87-A9
  - ***HardwareDriverID***
    A numerical ID used for identifying which video device driver to use for the hardware device in question. For information about how to find the right ID for your devices, see Hardware Driver IDs.
  - ***HardwarePort***
    Port to use for HTTP communication with the hardware device. Default is port 80.
  - ***HardwarePassword***
    Password for the hardware device's administrator account. For security reasons most organizations use their own passwords rather than device manufacturers' passwords.

  ### Optional Parameters

  You can furthermore include these optional parameters, regardless whether cameras and server are online or offline:

  - ***HardwareUserName*** and ***HardwarePassword***
    User name for the hardware device's administrator account. If you do not specify a user name, RC-P will use the device manufacturer's default user name for each hardware device. Many organizations use the hardware device manufacturers' default user names for their hardware devices. If that is the case in your organization, there is no need to painstakingly type hardware device manufacturers' default user names as this can be a source of error; trust that RC-P will know the manufacturers' default user names. Note that you must always specify a password (the *HardwarePassword* parameter) even when it is not necessary to specify user name.

    If the extremely rare cases where the user name for a hardware device is [blank], you cannot use the CSV method, since the method interprets no password as “use the hardware device manufacturer's default password.” If the user name for a hardware device is [blank], use the wizard's *Manual* method instead; with the *Manual* method you can use a [blank] user name.
  - ***HardwareDeviceName***
    Name of the hardware device. Name must unique, and must not contain any of the following special characters: < > & ' " \ / : * ? | [ ]
  - ***CameraName[number]***
    Name of the camera. Must appear as *CameraName1*, *CameraName2*, etc. in the header line since a hardware device can potentially have more than one camera attached. Names must unique, and must not contain any of the following special characters: < > & ' " \ / : * ? | [ ]
  - ***CameraShortcut[number]***
    Number for keyboard shortcut access to the camera in the Ocularis Client. Must appear as *CameraShortcut1*, *CameraShortcut2*, etc. in the header line since a hardware device can potentially

have more than one camera attached. A camera shortcut number must not contain any letters or special characters, and must not be longer than eight digits.

- ***PreBufferLength[optional number]***
  Required length (in seconds) of pre-recording. If specified as, for example, *PreBufferLength1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***PostBufferLength[optional number]***
  Required length (in seconds) of post-recording. If specified as, for example, *PostBufferLength1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***RecordingPath[optional number]***
  Path to the folder in which a camera's database should be stored. If specified as, for example, *RecordingPath1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***ArchivePath[optional number]***
  Path to the folder in which the camera's archived recordings should be stored. Remember that an archiving path is only relevant if not using dynamic paths for archiving. If specified as, for example, *ArchivePath1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***RetentionTime[optional number]***
  Required retention time (in minutes). Remember that retention time is the total of recording time plus archiving time. If specified as, for example, *RetentionTime1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***MjpegLiveFrameRate[optional number]***
  Required MJPEG live frame rate (in number of frames; depending on what has been configured on the camera, it will then know whether it is frames per second, minute, or hour). If specified as, for example, *MjpegLiveFrameRate1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***MjpegRecordingFrameRate[optional number]***
  Required MJPEG recording frame rate (in number of frames; depending on what has been configured on the camera, it will then know whether it is frames per second, minute, or hour). If you need to specify a value which includes a decimal separator, use the full stop character (example: 7.62). If specified as, for example, *MjpegRecordingFrameRate1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***MotionSensitivity[optional number]***
  A value between 0-256; corresponds to using the *Sensitivity* slider when configuring motion detection settings in the Management Application. If specified as, for example, *MotionSensitivity1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***MotionDetectionThreshold[optional number]***
  A value between 0-10000; corresponds to using the *Motion* slider when configuring motion detection settings in the Management Application. If specified as, for example, *MotionDetectionThreshold1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***MotionDetectionInterval[optional number]***
  Lets you specify how often motion detection analysis should be carried out on video from the camera. Specified in milliseconds. The interval is applied regardless of the camera's frame rate settings. If specified as, for example, *MotionDetectionInterval1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.

Most system integrators store hardware device information in spreadsheets like Microsoft Excel, from which they can save the information as comma-separated values in a CSV file. These examples show hardware information in Excel (1) and when exported to a CSV file (2); note the header lines:

1

	A	B	C
1	HardwareAddress	HardwareUsername	HardwarePassword
2	192.168.200.220	AdminAccountUserName	t0p5eCR3tpa55w0rd
3	192.168.200.221	AdminAccountUserName	TOPsecretPASSword
4	192.168.200.222	RootaccountUserName	ToPsEcReTpAsSwOrD
5	192.168.200.223	AdminAccountUserName	T0PS3Cr3Tpa5Sw0rD

2

```
HardwareAddress;HardwareUsername;HardwarePassword;Har
192.168.200.220;AdminAccountUserName;t0p5eCR3tpa55w0
192.168.200.221;AdminAccountUserName;TOPsecretPASSwo
192.168.200.222;RootaccountUserName;ToPsEcReTpAsSwOr
192.168.200.223;AdminAccountUserName;T0PS3Cr3Tpa5Sw0
```

Whichever method is used, the following applies:

- The first line of the CSV file must contain the headers, and subsequent lines must contain information about one hardware device each
- Separators can be commas, semicolons or tabs, but cannot be mixed
- All lines must contain valid values—pay special attention to the fact that camera names, user names, etc. must be unique, and must not contain any of the following special characters: < > & ' " \ / : * ? | [ ]
- There is no fixed order of values, and optional parameters can be omitted entirely
- Boolean fields are considered true unless set to 0, false or no
- Lines containing only separators are ignored
- Empty lines are ignored
- Even though the CSV file format is generally ASCII only, Unicode identifiers are allowed; even without Unicode identifiers, the entire file or even individual characters are allowed to be Unicode strings

If you need to include separator characters in a value—for example if a camera name is Reception; Camera 1—you can encapsulate the value in quotes to indicate that the separator should not be interpreted as separating values in the file. Such quote-encapsulated values are interpreted as they appear. If a separator, a quote or a space is needed in a value, the whole value has to be encapsulated in quotes. Leading and trailing spaces outside the quote-encapsulated value are removed, while spaces inside the quote-encapsulated value are maintained. No characters (except spaces) are allowed outside the quote-encapsulated value. A double quote inside a quote-encapsulated value is interpreted as a single quote. Nested quotes (quotes inside quotes) are not allowed.

Some examples (using semicolon as the separator):

- "camera"; is interpreted as camera
- "cam;""era"; is interpreted as cam;"era
- """"camera""""; is interpreted as "camera"
- ""; is interpreted as an empty string
- ...; " cam"" era " ;... is interpreted as | cam" era | (where | is not part of the interpretation but only used to show the start and end of the interpretation)
- ""camera; is not valid as there are characters outside the quote-encapsulated value
- "cam" "era"; is not valid as the two quotes are separated with a space and quotes cannot be nested
- "cam"er"a"; is not valid as you cannot nest quotes
- cam"era"; is not valid as there are characters outside the quotes

Replace Hardware Device Wizard

The Replace Hardware Device wizard helps you replace a hardware device—which you have previously added to and configured on your surveillance system—with a new one. The wizard is divided into two pages:

- New Hardware Device Information
- Database Action

Remember that you must have a Device License Key (DLK) for every hardware device (cameras, etc.) you intend to use on your RC-P system. Before using the wizard, make sure you have a DLK for the new hardware device.

Properties: Name & Video Channels

- ***Hardware name*:** Name of the hardware device as it will appear in the Management Application. If required, you can overwrite the existing hardware device name with a new one. Hardware device names must be unique, and must not contain any of the following special characters: < > & ' " \ / : * ? | [ ]

- ***Video channel # enabled*:** Lets you enable/disable each of the selected hardware device's video channels. Many hardware devices only have a single video channel, in which case only one channel will be listed. Other hardware devices—typically video encoder devices—have several video channels.

  Why are some of the channels unavailable? This will be the case if you are not licensed to use all of a video encoder device's channels. Example: You have a video encoder device with four channels, but your license for the device only allows you to use two of them. In that case, you will only be able to have two channels enabled at a time; the two other channels will be disabled. Note that you are free to select which two channels you want to enable. Contact OnSSI if you need to change your number of licenses.

Network, Device Type & License

When configuring hardware devices, specify the following properties:

- ***Address*:** IP address or host name of the hardware device.
- ***HTTP port*:** Port to use for HTTP communication with the hardware device. Default is port 80. To use the default port, select ***Use default HTTP port***.
- ***FTP port*:** Port to use for FTP communication with the hardware device. Default is port 21. To use the default port, select ***Use default FTP port***.
- ***User name*:** User name for the hardware device's administrator account. Many organizations use the hardware device manufacturer's default user names for their hardware devices. If that is the case in your organization, select <*default*> (do not type a manufacturer's default user name as this can be a source of error; trust that RC-P will know the manufacturer's default user name). Other typical user names, such as *admin* or *root* are also selectable from the list. If requiring a user name which is not on the list, simply type the required user name.
- ***Password*:** Password for the hardware device's administrator account, a.k.a. the root password.
- ***Hardware type*:** Read-only field displaying the type of video device driver used for communication with the hardware device.
- ***Serial number (MAC address)*:** Read-only field displaying the serial number of device. The serial number is usually identical to the 12-character hexadecimal MAC address of the hardware device (example: 0123456789AF).
- ***Device license key (DLK)*:** The 16-character license key (DLK) which gives you the right to use the hardware device with RC-P.
- ***Replace Hardware Device*:** Opens a wizard, with which you—if required—can replace the selected hardware device with another one. This can typically be relevant if you replace a physical camera on your network. The wizard helps you take all relevant issues into account: finding the DLK for the new hardware device, deciding what to do with recordings from cameras attached to the old hardware device, etc.

PTZ Device

The *PTZ Device* tab is only available if configuring video encoder hardware devices on which the use of PTZ (Pan/Tilt/Zoom) cameras is possible:

- ***Connected cameras have Pan/tilt/Zoom capabilities*:** Select check box if any of the cameras attached to the video encoder device is a PTZ camera.
- ***PTZ type on COM#*:** If a PTZ camera is controlled through the COM port (a.k.a. serial port) in question, select the required option. Options are device-specific, depending on which PTZ protocols are used by the device in question. If no PTZ cameras are controlled through the COM port in question, select *None*.

  Some of the options concern absolute and relative positioning. What is that? Absolute positioning is when the PTZ camera is controlled based on a single fixed position, against which all other positions are measured. Relative positioning is when the PTZ camera is controlled relative to its current position.

The table in the lower half of the dialog contains a row for each video channel on the hardware device. First row from the top corresponds to video channel 1, second row from the top corresponds to video channel 2, etc.

- ***Name*:** Name of the camera attached to the video channel in question.
- ***Type*:** Lets you select whether the camera on the selected camera channel is fixed or moveable:
  - ***Fixed*:** Camera is a regular camera mounted in a fixed position
  - ***Moveable*:** Camera is a PTZ camera
- ***Port*:** Available only if *Moveable* is selected in the *Type* column. Lets you select which COM port on the video encoder to use for controlling the PTZ camera.
- ***Port Address*:** Available only if *Moveable* is selected in the *Type* column. Lets you specify port address of the camera. The port address will normally be *1*. If using daisy chained PTZ cameras, the port address will identify each of them, and you should verify your settings with those recommended in the documentation for the camera.

Licenses

Import DLKs (Device License Keys)

You must have a Device License Key (DLK) for every hardware device (cameras, etc.) on your RC-P system.

Remember that you are allowed to install and use only the number of cameras covered by your license agreement; regardless of your number of available DLKs. For example, a fully used four-port video encoder counts as four cameras; it will thus use four licenses even though its four cameras are connected through a single hardware device.

You get DLKs as part of the software registration process. Upon registration, all your DLKs are sent to you as a single .dlk file attached to an e-mail.

Importing the file is quick and easy, and it will free you from having to specify license keys manually for each hardware device later.

1. When you receive the e-mail, save the attached .dlk file at a location accessible from the RC-P server, for example on a network drive or on a USB stick.

2. In the Management Application's *File* menu, select *Import DLKs...* (or click the *Import DLKs* button if you are working with the Add Hardware Devices wizard).

   If you need to import DLKs in connection with an upgrade of your RC-P software version, always use the *File* > *Import DLKs...* method.

3. Browse to the location at which you have saved the received .dlk file, select the file, and click *Open*. All DLKs are now imported into RC-P, and will be available when you add cameras and other hardware.

Specify a New SLC (Software License Code)

SLCs are required for both the recording component (RC-P) and the Ocularis Base component. Each SLC is entered in a different location.

Ocularis Base SLC

This SLC is entered in the *Ocularis Licensing Activation* application. See the *Ocularis Installation & Licensing Guide* for further instructions.

Recording Component (RC-P) SLC

If you need to add a new Software License Code (SLC) to RC-P, do the following:

1. In the Management Application's *Help* menu, select *About...*

2. In the *Software License Code (SLC)* field, enter the SLC (or overwrite the existing SLC with the new SLC), and click *OK*.

3. You must close the Management Application. When you open the Management Application again, the new SLC will take effect.

Logging

Overview of Logs

The RC-P recording component is able to generate various logs:

- ### Log Types

  - **Management Application log files.** These files log activity in the Management Application. A new log file is created for each day the Management Application is used. You cannot disable this type of logging. Management Application log files are named according to the structure AdminYYYYMMDD.log, for example Admin20101231.log.

  - **Recording Server service log files.** These files log Recording Server service activity. A new log file is created for each day the service is used. You cannot disable this type of logging. Recording Server service log files are named according to the structure RecordingServerYYYYMMDD.log, for example RecordingServer20101231.log.

  - **Image Server service log files.** These files log activity on the Image Server service. A new log file is created for each day the service is used. You cannot disable this type of logging. Image Server service log files are named according to the structure ISLog_YYYYMMDD.log, for example ISLog_20101231.log.

  - **Image Import service log files.** These files log activity regarding the Image Import service, when this service is used for fetching pre-alarm images, and storing the fetched images in camera databases. Pre-alarm images is a feature available for selected cameras only; it enables sending of images from immediately before an event took place from the camera to the surveillance system via e-mail. A new log file is created for each day the service is used. You cannot disable this type of logging. Image Import service log files are named according to the structure ImageImportLog_YYYMMDD.log, for example ImageImportLog20101231.log.

  - **Event log files.** These files log information about registered events. A new log file is created for each day on which events occur. You cannot disable this type of logging.

  - **Audit log files:** These files log Ocularis Client user activity provided audit logging is enabled. A new log file is created for each day with audit logging enabled and client user activity. Audit log files are named according to the structure is_auditYYYMMDD.log, for example is_audit20101231.log. The _is prefix is due to the fact that the audit log files are generated by the Image Server service.

- ### Log Locations

  By default, all log files are placed in the appropriate *All Users* folder for the operating system used, for example C:\ProgramData\OnSSI\Recorders\RC-P if running Windows Vista. They are stored for seven days by default. Note, however, that log file locations as well as the number of days to store the logs can be changed as part of the logging configuration.

- ### Log Structures

  Most log files generated by RC-P use a shared structure complying with the W3C Extended Log File Format. Each log file consists of a header and a number of log lines:

  - The header outlines the information contained in the log lines.

  - The log lines consist of two main parts: the log information itself as well as an encrypted part. The encrypted part makes it possible—through decryption and comparison—to assert that a log file has not been tampered with.

- ### Log Integrity Checks

  All log files, except Management Application log files, are subjected to an integrity check once every 24 hours. The integrity check is performed by RC-P's Log Check service.

The result of the integrity check is automatically written to a file named according to the structure LogCheck_YYYYMMDD.log, for example LogCheck_20101231.log. Like the log files themselves, the log check files are by default placed in the appropriate All Users folder for the operating system used, for example C:\ProgramData\OnSSI\<NVR_Name> if running Windows Vista.

Any inconsistencies will be reported in the form of error messages written in the log check file. Possible error messages (other, non-error, messages may also appear in the log check file):

- ***Log integrity information was not found. Log integrity can't be guaranteed.*:** The log file could not be checked for integrity.
- ***Log information does not match integrity information. Log integrity can't be guaranteed.*:** The log file exists, but does not contain the expected information. Thus, log integrity cannot be guaranteed.
- ***[Log file name] not found*:** The log file was not present.
- ***[Log file name] is empty*:** The log file was present, but empty.
- ***Last line changed/removed in [log file name]*:** The last line of the log file did not match validation criteria.
- ***Encrypted data missing in [log file name] near line [#]*:** The encrypted part of the log line in question was not present.
- ***Inconsistency found in [log file name] near line [#]*:** The log line does not match the encrypted part.
- ***Inconsistency found in [log file name] at beginning of log file*:** The log file header is not correct. This situation is most likely to occur if a user has attempted to delete the beginning of a log file.

Configure System, Event and Audit Logging

RC-P is able to generate various logs. To configure logging, do the following:

1. In the Management Application's Navigation pane, expand *Advanced Configuration*, right-click *Logs* and select *Properties*.
2. Specify required properties for:
   - General system logs (Management Application log, Recording Server service log, Image Server service log, Image Import service log)
   - The event log
   - The audit log

   Note that only audit logging can be disabled/enabled by administrators; all other logs are compulsory. When ready, click *OK*.
3. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

Properties: Logs

Logs (that is Management Application log, Recording Server service log, Image Server service log, Image Import service log)

- ***Path*:** These system log files are by default placed in the appropriate *All Users* folder for the operating system used, for example C:\ProgramData\OnSSI\RC-P if running Windows Vista. To specify another location for your log files, type the path to the required folder in the *Path* field, or click the browse button next to the field to browse to the required folder.
- ***Days to log*:** A new log file is created each day the Management Application and/or the services are used. A log file older than the number of days specified in the field is automatically deleted. By default, the log file will be

stored for seven days. To specify another number of days (max. 9999), simply overwrite the value in the field. The current day's activity is always logged, even with a value of 0 in the field. Therefore, if you specify 0, you will log current day's activity; if you specify 1, you will keep one day plus the current day's activity, and so on.

Event Log

- ***Path*:** Event log files are by default placed in the appropriate *All Users* folder for the operating system used, for example C:\ProgramData\OnSSI\RC-P if running Windows Vista. To specify another location for your event log files, type the path to the required folder in the *Path* field, or click the browse button next to the field to browse to the required folder.

- ***Days to log*:** A new log file is created for each day on which events occur. A log file older than the number of days specified in the field is automatically deleted. By default, the log file will be stored for seven days. To specify another number of days (max. 9999), simply overwrite the value in the field. The current day's activity is always logged, even with a value of 0 in the field. Therefore, if you specify 0, you will log current day's activity; if you specify 1, you will keep one day plus the current day's activity, and so on.

Audit Log

- ***Enable audit logging*:** Audit logging is the only type of RC-P logging which is not compulsory. Select/clear the check box to enable/disable audit logging.

- ***Path*:** Audit log files are by default placed in the appropriate *All Users* folder for the operating system used, for example C:\ProgramData\OnSSI\RC-P if running Windows Vista. To specify another location for your audit log files, type the path to the required folder in the *Path* field, or click the browse button next to the field to browse to the required folder.

- ***Days to log*:** A new log file is created for each day with audit logging enabled and client user activity. A log file older than the number of days specified in the field is automatically deleted. By default, the log file will be stored for seven days. To specify another number of days (max. 9999), simply overwrite the value in the field. The current day's activity is always logged (provided audit logging is enabled and there is user activity). Therefore, if you specify 1, you will keep one day plus the current day's activity. Note that if you specify 0 (zero), audit log files will be kept indefinitely (disk space permitting).

- ***Minimum logging interval*:** Minimum number of seconds between logged events. Specifying a high number of seconds between logged events may help reduce the size of the audit log. Default is 60 seconds.

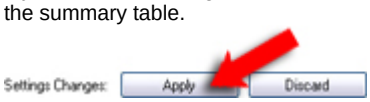
- ***In sequence timespan*:** Number of seconds to pass for viewed images to be considered to be within the same sequence. Specifying a high number of seconds may help limit the number of viewed sequences logged, and thus reduce the size of the audit log. Default is ten seconds.

Management Application

Apply or Save Configuration Changes

Whenever you make changes in your RC-P configuration, you will be asked to apply them:

- If you made the changes in one of the Management Application's dialogs, you simply apply them by clicking *OK*.
- If you made the changes in one of the Management Application's summary tables, click the *Apply* button below the summary table.



Applying a configuration change means that the change is stored by RC-P in a restore point (so that you can return to a working configuration if something goes wrong), but **applying a configuration change does not mean that the changes will take immediate effect** on the surveillance system.

- To actually store your configuration change in RC-P's configuration file, click the *Save Configuration* button in the Management Application's toolbar (or select *File* > *Save* from the menu). Your configuration changes will then take effect the next time RC-P's services are restarted.
- If you want your configuration changes to have immediate effect, RC-P's services must be restarted: Click the *Save Changes and Restart Surveillance Services* button in the Management Application's toolbar (or select *File* > *Save Changes and Restart Services* from the menu).

IMPORTANT: While services are restarted, it will not be possible to view or record video. Restarting the services typically only takes some seconds, but in order to minimize disruption you may want to restart services at a time when you do not expect important incidents. Users connected to RC-P through clients will typically remain logged in during the services restart, but they will experience a short video outage.

Change or Reset Management Application Behavior

You can change the way the Management Application behaves. For example, the Management Application will ask you to confirm many of your actions by default. If you find this annoying, you can change the Management Application's behavior, so it will not ask you again.

1. In the Management Application's menu bar, select *Application Settings* > *Application Behavior...*
2. For each action, you can now select how the Management Application should behave. Examples:
   - When you attempt to delete a hardware device, should the Management Application ask you to confirm that you want to delete the hardware device, or should it delete the hardware device straight away without asking?
   - You can use a maximum of 64 cameras at a time on a single RC-P server. If you add more than 64 cameras, should the Management Application warn you or not?

   Note that selectable behavior may vary, depending on the type of action
3. Click *OK*.
4. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

Configure the Management Application Password Protection

By default, anyone who is able to log in to the RC-P server is able to use the Management Application. The reason for this is that such people are likely to have administrator rights.

If required, you can password protect access to the Management Application for additional security:

1. In the Management Application's navigation pane, expand *Advanced Configuration*, expand *Users*, right-click *Administrator*, and select *Properties*.

2. Under *Management protection*, select *Enable*.

3. Specify required password, and repeat it to be sure you have specified it correctly.

   Only use the *Old password* field if changing an existing password or disabling management protection, in which case the old password is required to prove that you have the rights to make the changes.

5. Click *OK*.

6. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

Scheduling

Configure General Scheduling and Archiving

RC-P's general Scheduling and Archiving feature lets you configure when:

- Cameras should be online (that is transfer video to RC-P)
- Cameras should use speedup (that is use a higher than normal frame rate)
- You want to receive any e-mail notifications regarding cameras
- Archiving should take place

Do the following:

1. In the Management Application's navigation pane, expand *Advanced Configuration*, right-click *Scheduling and Archiving*, and select *Properties*.
2. Specify properties as required for Scheduling All Cameras, Scheduling Options, and Archiving. When ready, click *OK*.
3. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

Configure Camera-specific Schedules

With camera-specific scheduling, you can configure when:

- A camera should be online (that is transfer video to RC-P)
- A camera should use speedup (that is use a higher than normal frame rate)
- You want to receive any e-mail notifications regarding the camera

Do the following:

1. In the Management Application's navigation pane, expand *Advanced Configuration*, expand *Scheduling and Archiving*, right-click the required camera, and select *Properties*.
2. Specify properties as required for Online Period, Speedup, E-mail Notification. When ready, click *OK*.
3. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

General Scheduling Properties

Scheduling All Cameras

All properties on a white background are editable, properties on a light blue background cannot be edited. Note that the properties Online Period, Speedup, E-mail Notification can also be specified individually for each camera.

- ***Template*:** The template can help you configure similar properties quickly. For examples: you have 50 cameras and you want to change the online schedule profile for all of them. Instead of having to select the same 50 times, you can simply enter them once in the template, and then apply the template to the 50 cameras with only two clicks.
- ***Apply Template*:** Lets you select which cameras you want to apply the template for. You then use one of the two *Set* buttons (see descriptions in the following) to actually apply the template.
- ***Camera*:** Name of each camera as it will appear in the Management Application as well as in clients.
- ***Online*:** Lets you select the required profile (for example *Always on*) for the online schedule for the camera(s) in question.
- ***Speedup*:** Lets you select the required profile for the speedup schedule for the camera(s) in question.
- ***E-mail*:** Lets you select the required profile for the e-mail notification schedule for the camera(s) in question.
- ***Select All*:** Click button to select all cameras in the *Apply Template* column.
- ***Clear All*:** Click button to clear all selections in the *Apply Template* column
- ***Set selected template value on selected cameras*:** Lets you apply only a selected value from the template to selected cameras.
- ***New schedule profile*:** Lets you create a new schedule profile of any type by clicking the ***Create...*** button.

Scheduling Options

- ***Start cameras on client requests*:** Cameras may be offline, for example because they have reached the end of an online schedule, in which case client users will not be able to view live video from the cameras. However, if you select *Start cameras on client requests*, client users will be able to start the camera (technically: force the camera to be online outside its online schedule) in order to view live video from the camera.
- ***Schedule profile for new cameras*:** Lets you select which online schedule profile to use as default for cameras you subsequently add to your RC-P system. Note that your selection only applies for the online schedule, not for any other schedules. Default selection is *Always on*, meaning that new cameras will always be online, that is transferring video to the RC-P server for live viewing and further processing.
- ***Maximum delay between reconnect attempts*:** Lets you control the aggressiveness of reconnection attempts. If RC-P loses the connection to a camera, it will by default attempt to re-establish the connection after ten seconds. In some environments, for example if using vehicle-mounted cameras through wireless connections, camera connections may frequently be lost, and you may want to change the aggressiveness of such reconnection attempts.

Archiving

RC-P automatically archives recordings if a camera's database becomes full (in earlier versions, this was an option configured individually for each camera).

You are furthermore able to schedule archiving at particular points in time every day. This way, you can proactively archive recordings, so databases will never become full. As a rule of thumb, the more you expect to record, the more often you should archive.

- ### Archiving Time

  The *Archiving Times* list shows the times at which you want to automatically archive the content of all camera databases on your RC-P server. You can do this up to 24 times per day, with minimum one hour between each one.

  To add archiving times to the list:

  1. Specify required time in the time box to the right of the *Archiving Times* list. You specify the required time by selecting the hour, minute and second values respectively, then clicking the *up* and *down* buttons to increase or decrease values. Alternatively, you can simply overwrite selected hour, minute or second values.
  2. Click the *Add* button.

- ### Archive Failure Notification

  You can automatically get notified if archiving fails:

  - ***Send e-mail on archiving failure*:** If selected, RC-P will automatically send an e-mail to selected recipients if archiving fails. This requires that the e-mail notification feature is enabled. Recipients are defined as part of the e-mail notification properties.

  E-mail and SMS notifications are normally only sent during scheduled periods. However, archiving failures are considered to be so serious that, if enabled, e-mail notifications regarding archiving failures are sent regardless of schedules.

Camera-specific Scheduling Properties

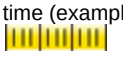
Online Period

When you configure scheduling for specific cameras, your *Online Period* settings are probably the most important, since they determine when each camera should transfer video to RC-P.

By default, cameras added to RC-P will automatically be online, and you will only need to modify the online period settings if you require cameras to be online only at specific times or events. Note, however, that this default may be changed as part of the general scheduling options, in which case subsequently added cameras will not automatically be online.

The fact that a camera transfers video to RC-P does not necessarily mean that video from the camera is recorded. Recording is configured separately; see Configure Video & Recording.

You specify a camera's online periods by creating schedule profiles based on:

- Periods of time (example: Mondays from 08.30 until 17.45), shown in pink:
- Events within periods of time (example: from Event A occurs until Event B occurs Mondays from 08.30 until 17.45), shown in yellow: 

The two options can be combined , but they cannot overlap in time.

RC-P comes with two simple schedule profiles, ***Always on*** and ***Always off***, which cannot be edited or deleted. If these do not meet your needs, you can create any number of customized schedule profiles for each camera. When you create a customized schedule profile for one camera, you can reuse it with other cameras if required. To create a customized schedule profile:

1. In the field below the ***Schedule profiles*** list, specify a name for the new schedule profile. Schedule profile names must not contain any of the following special characters: < > & ' " \ / : * ? | [ ]

2. Click the ***Add New*** button (which becomes available when you specify a name).

3. In the top right corner of the dialog, select ***Set camera to start/stop on time*** (to base subsequent settings on periods of time) or ***Set camera to start/stop on event*** (to base subsequent settings on events within periods of time).

4. In the calendar section, place your mouse pointer at a required start point, then hold down the left mouse button, drag the mouse pointer and release at the required end point.

    - You specify each day separately.

    - You specify time in increments of five minutes; RC-P helps you by showing the time over which your mouse pointer is positioned:

    - If you base your schedule profile—or parts of it—on events within periods of time, remember to select ***Start event*** and ***Stop event*** from the lists below the calendar section.

    - To delete an unwanted part of a schedule profile, right-click it and select *Delete*.

    - To quickly fill or clear an entire day, double-click the name of the day.

    - As an alternative to dragging inside the calendar section, use the ***Start time***, ***End time*** and ***Day*** fields, then the ***Change Period*** or ***Set Period*** button as required. When using the *Start time* and *End time* fields, remember that time is specified in increments of five minutes. You cannot specify a period shorter than five minutes, and you can only use times like 12:00, 12.05, 12:10, 12:15, etc. If you specify a time outside of the five-minute intervals, such as 12:13, you will get an error message.

Speedup

When you configure scheduling for specific MJPEG cameras, you can specify speedup periods. Before you can define this type of schedule, speedup must be enabled. You specify a camera's speedup periods by creating schedule profiles based on:

- Periods of time (example: Mondays from 08.30 until 17.45), shown in olive green:

Speedup may also take place based on events, but that is configured elsewhere: See Frame Rate - MJPEG (General Recording & Storage Properties) and Frame Rate (Camera-specific Properties).

RC-P comes with two simple schedule profiles, ***Always on*** and ***Always off***, which cannot be edited or deleted. If these do not meet your needs, you can create any number of customized schedule profiles for each camera. When you create a customized schedule profile for one camera, you can reuse it with other cameras if required. To create a customized schedule profile:

1. In the field below the ***Schedule profiles*** list, specify a name for the new schedule profile. Schedule profile names not contain any of the following special characters: < > & ' " \ / : * ? | [ ]

2. Click the ***Add New*** button (which becomes available when you specify a name).

3. In the calendar section, place your mouse pointer at a required start point, then hold down the left mouse button, drag the mouse pointer and release at the required end point.

    - You specify each day separately.

    - You specify time in increments of five minutes; RC-P helps you by showing the time over which your mouse pointer is positioned:

    - To delete an unwanted part of a schedule profile, right-click it and select *Delete*.

- To quickly fill or clear an entire day, double-click the name of the day.

- As an alternative to dragging inside the calendar section, use the ***Start time***, ***End time*** and ***Day*** fields, then the ***Change Period*** or ***Set Period*** button as required. When using the *Start time* and *End time* fields, remember that time is specified in increments of five minutes. You cannot specify a period shorter than five minutes, and you can only use times like 12:00, 12.05, 12:10, 12:15, etc. If you specify a time outside of the five-minute intervals, such as 12:13, you will get an error message.

E-Mail Notification

When you configure scheduling for specific cameras, you can specify e-mail notification periods. Before you can define this type of schedule, e-mail notification must be enabled. You specify a camera's e-mail notification periods by creating schedule profiles based on:

- Periods of time (example: Mondays from 08.30 until 17.45), shown in blue:

RC-P comes with two simple schedule profiles, ***Always on*** and ***Always off***, which cannot be edited or deleted. If these do not meet your needs, you can create any number of customized schedule profiles for each camera. When you create a customized schedule profile for one camera, you can reuse it with other cameras if required. To create a customized schedule profile:

1. In the field below the ***Schedule profiles*** list, specify a name for the new schedule profile. Schedule profile names not contain any of the following special characters: < > & ' " \ / : * ? | [ ]

2. Click the ***Add New*** button (which becomes available when you specify a name).

3. In the calendar section, place your mouse pointer at a required start point, then hold down the left mouse button, drag the mouse pointer and release at the required end point.

    - You specify each day separately.

    - You specify time in increments of five minutes; RC-P helps you by showing the time over which your mouse pointer is positioned:

    - To delete an unwanted part of a schedule profile, right-click it and select *Delete*.

    - To quickly fill or clear an entire day, double-click the name of the day.

    - As an alternative to dragging inside the calendar section, use the ***Start time***, ***End time*** and ***Day*** fields, then the ***Change Period*** or ***Set Period*** button as required. When using the *Start time* and *End time* fields, remember that time is specified in increments of five minutes. You cannot specify a period shorter than five minutes, and you can only use times like 12:00, 12.05, 12:10, 12:15, etc. If you specify a time outside of the five-minute intervals, such as 12:13, you will get an error message.

Services

Overview of Services

The following services are all automatically installed on the RC-P server:

- **RC-P Recording Server service:** A vital part of the surveillance system; video streams are only transferred to RC-P while the Recording Server service is running.
- **RC-P Image Server service:** Provides access to the surveillance system for users logging in with the Ocularis Client.
- **RC-P Image Import service:** Used for fetching pre- and post-alarm images, and storing the fetched images in camera databases. Pre- and post-alarm images is a feature available for selected cameras only; it enables sending of images from immediately before an event took place from the camera to the surveillance system via e-mail. Pre- and post-alarm images should not be confused with RC-P's own pre- and post-recording feature.
- **RC-P Log Check service:** Performs integrity checks on RC-P log files. For more information, see Overview of Logs.

The services by default run transparently in the background on the RC-P server. If required, you are able to start and stop each service separately from the Management Application; see Start & Stop Services.

Start & Stop Services

On an RC-P server, four services run in the background by default. If required, you can start and stop each service separately:

1. In the Management Application's Navigation pane, expand *Advanced Configuration* and select *Services*. This will display the status of each service.
2. You can now stop each service by clicking the *Stop* button. When a service is stopped, the button changes to *Start*, allowing you to start the service again when required.

System

Configure Default File Paths

RC-P uses a number of default file paths:

- ***Default recording path for new cameras*:** All new cameras you add will by default use this path for storing recordings. If required, you can change individual cameras' recording paths as part of their individual configuration, but you can also change the default recording path so all new cameras you add will use a path of your choice.

- ***Default archiving path for new cameras*:** All new cameras you add will by default use this path for archiving. If required, you can change individual cameras' archiving paths as part of their individual configuration, but you can also change the default recording path so all new cameras you add will use a path of your choice. Note that camera-specific archiving paths are not relevant if using dynamic path selection for archiving.

- ***Configuration path*:** The path by default used for storing your RC-P system's configuration.

To change any of the default file paths:

1. If changing the configuration path, stop all services. This step is not necessary if changing the default recording or archiving path.

2. In the Management Application's menu bar, select *Application Settings > Default File Paths...*

3. You can now overwrite required paths. Alternatively, click the browse button next to the required field and browse to the required location.

   For the default recording path, you are only able to specify a path to a folder on a *local* drive. If using a network drive, it would not be possible to save recordings if the network drive became unavailable.

   If you change the default recording or archiving paths, and there are existing recordings at the old locations, you will be asked whether you want to move the recordings to the new locations (recommended), leave them at the old locations, or delete them.

4. Click *OK*.

5. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

6. Restart all services.

Find Version & Plug-in Information

Knowing the exact version of your RC-P system can be important if you require support, want to upgrade your system, etc. In such cases, you may also want to know which plug-ins your RC-P system uses.

To view such information, select *About...* in the Management Application's *Help* menu.

System Restoration

Restore System Configuration from a Restore Point

Restore points allow you to return to a previous configuration state. Each time a configuration change is applied in the Management Application—either by clicking *OK* in a properties dialog or by clicking the *Apply* button in a summary pane—a new restore point is created.

All restore points in the current and previous five sessions are stored and can be selected again. A new session begins each time the Management Application is started as well as each time you save the whole configuration, for example by clicking the *Save Configuration* button in the Management Application's toolbar. For sessions older than the last five sessions, only the latest restore point of each session is stored. With the *Number of old sessions to keep* field you can control how many old sessions are kept.

When selecting to restore a configuration from a restore point, the configuration from the selected restore point will be applied and used once the services are restarted (see Start & Stop Services).

If you have added new cameras or other devices to RC-P after the restore point was created, they will be missing if you load the restore point. This is due to the fact that they were not in the system when the restore point was created. In such cases, you will be notified and must decide what to do with recordings from the affected devices.

1. From the Management Application's *File* menu, select *Load Configuration from Restore Point...*
2. In the left part of the *Restore Points* dialog, select the required restore point.
3. Click the *Load Restore Point* button.
4. If you are sure that you want to overwrite the current configuration with the one from the selected restore point, click *OK*.
5. Only relevant if the current configuration contains cameras or other devices which were not present in the selected restore point: You will be asked whether you want to delete or keep recordings from affected devices. If keeping the recordings, note that they will not be accessible until you add the affected devices to RC-P again. Select the required option, and click *OK*.
6. Click *OK* in the Restore Points dialog.
7. In the Management Application's navigation pane, expand *Advanced Configuration*, and select *Services*.
8. For the Recording Server and Image Server services respectively, click the *Restart* button. When the two services are restarted, the configuration from the selected restore point is applied.

Export & Import System Configuration

You can export the current configuration of your RC-P system, either as a safety measure in order to have a backup file of your configuration, or a as a clone allowing you to use a similar configuration elsewhere. You are subsequently able to import previously exported configurations.

- ### Export Configuration as Backup

  With this option, all relevant RC-P configuration files will be combined into one single file, which can then be saved at a location specified by you. Note that if there are unsaved changes to your configuration, they will automatically be saved when you export the configuration.

  1. In the Management Application's *File* menu, select *Export Configuration - Backup*.
  2. Browse to the location at which you want to store the exported configuration, specify a suitable file name, and click *Save*.

  If you intend to set up an identical version of your surveillance system elsewhere, **do not** export your configuration as *backup*, since this may lead to the same device information being used twice, in which case clients may get the following error message: *Application is not able to start because two (or more) cameras are using the same name or id.* Instead, export your configuration as a *clone*. When you export as a clone, the export takes into account the fact that you will not use the exact same physical cameras, etc. even though your new system may otherwise be identical to your existing one.

- ### Export Configuration as Clone

  With this option, all relevant RC-P configuration files will be collected, and GUIDs (Globally Unique IDentifiers; unique 128-bit numbers used for identifying individual system components, such as cameras) will be marked for later replacement.

  Why are GUIDs marked for replacement? GUIDs are marked for later replacement because they refer to specific components (cameras, etc.). Even though you wish to use the cloned configuration for setting up a new similar system using similar types of cameras, the new system will not use the exact same physical cameras as the cloned system. When the cloned configuration is later used in a new system, the GUIDs will therefore be replaced with GUIDs representing the specific components of the new system.

  After GUIDs have been marked for replacement, the configuration files will be combined into one single file, which can then be saved at a location specified by you. Note that if there are unsaved changes to your configuration, they will automatically be saved when you export the configuration.

  1. In the Management Application's *File* menu, select *Export Configuration - Clone*.
  2. Browse to the location at which you want to store the exported configuration, specify a suitable file name, and click *Save*.

- ### Import Previously Exported Configuration

  The same import method is used regardless of whether the configuration was exported as a backup or a clone.

  1. In the Management Application's *File* menu, select *Import Configuration*.
  2. Browse to the location from which you want to import the configuration, select the required configuration file, and click *Open*.
  3. Only relevant if the system into which you import the configuration contains devices (cameras, etc.) which are not present in the imported configuration: You will be asked whether you want to delete or keep recordings from affected devices. If keeping the recordings, note that they will not be accessible until you add the affected devices to RC-P again. Select the required option, and click *OK*.
  4. In the Management Application's navigation pane, expand *Advanced Configuration*, and select *Services*.
  5. For the Recording Server and Image Server services respectively, click the *Restart* button. When the two services are restarted, the imported configuration is applied.

Import Changes to Configuration

It is possible to import changes to a configuration. This can be relevant if installing many similar RC-P systems, for example in a chain of shops where the same types of server, hardware devices, and cameras are used in each shop. In such cases, you can use an existing configuration—typically a cloned configuration—as a template for the other installations. However, since the shops' installations are not exactly the same (the hardware devices and cameras are of the same type, but they are not physically the same, and thus they have different MAC addresses), there needs to be an easy way of importing changes to the template configuration.

This is why RC-P lets you import changes about hardware devices and cameras as comma-separated values (CSV) from a file:

1. From RC-P's menu bar, select *File > Import Changes to Configuration...*
2. Select *Online verification* if the new hardware devices and cameras listed in your CSV file are connected to the server and you want to verify that they can be reached.
3. Then point to the CSV file, and click the *Import Configuration from File* button.

- ### CSV File Format and Requirements

  The CSV file must have a header line (determining what each value on the subsequent lines is about), and subsequent lines must each contain information about one hardware device only.

  A minimum of information is always required for each hardware device:

  - ***HardwareOldMacAddress***
    The MAC address of the hardware device used in the template configuration. Required format: 12

hex characters without spaces or six groups of two hex characters separated with dashes (-) or colons (:).

You can furthermore include these optional parameters:

- ***HardwareNewMacAddress***
  The MAC address of the new hardware device to be used in the real configuration. Required format: 12 hex characters without spaces or six groups of two hex characters separated with dashes (-) or colons (:).
- ***HardwareAddress***
  IP address of the hardware device. Required format: IPv4 or IPv6.
- ***HardwareUsername***
  User name for hardware device's administrator account.

  In the extremely rare cases where a particular user name has previously been required for a device, but you now want the user name to be <blank>, you cannot use the CSV file to specify <blank>. The reason is that no information is interpreted as “leave the user name as it currently is.” If you need the new user name to be <blank>, you should not change it through the CCV file. Instead, change it as part of the hardware device's Network, Device Type & License properties after you have imported the other changes through the CSV file.
- ***HardwarePassword***
  Password for hardware device's administrator account.

  In the extremely rare cases where a particular password has previously been required for a device, but you now want the password to be <blank>, you cannot use the CSV file to specify <blank>. The reason is that no information is interpreted as “leave the password as it currently is.” If you need the new password to be <blank>, you should not change it through the CSV file. Instead, change it as part of the hardware device's Network, Device Type & License properties after you have imported the other changes through the CSV file.
- ***DLK***
  Device License Key (DLK) required in order to use the hardware device with RC-P.
- ***HardwareDeviceName***
  Name of the hardware device. Name must unique, and must not contain any of the following special characters: < > & ' " \ / : * ? | [ ]
- ***CameraName[number]***
  Name of the camera. Must appear as *CameraName1*, *CameraName2*, etc. in the header line since a hardware device can potentially have more than one camera attached. Names must be unique, and must not contain any of the following special characters: < > & ' " \ / : * ? | [ ]
- ***CameraShortcut[number]***
  Number for keyboard shortcut access to the camera in the Ocularis Client. Must appear as *CameraShortcut1*, *CameraShortcut2*, etc. in the header line since a hardware device can potentially have more than one camera attached. A camera shortcut number must not contain any letters or special characters, and must not be longer than eight digits.
- ***GenerateNewCameraGuid[optional number]***
  Lets you specify whether to generate a new GUID for a camera; this is especially relevant if using a cloned configuration as your template, since all GUIDs are removed from cloned configurations. If specified as, for example, *GenerateNewCameraGuid1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device. Any character means “yes, generate a new GUID.”
- ***PreBufferLength[optional number]***
  Required length (in seconds) of pre-recording. If specified as, for example, *PreBufferLength1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***PostBufferLength[optional number]***
  Required length (in seconds) of post-recording. If specified as, for example, *PostBufferLength1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***RecordingPath[optional number]***
  Path to the folder in which a camera's database should be stored. If specified as, for example, *RecordingPath1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***ArchivePath[optional number]***
  Path to the folder in which the camera's archived recordings should be stored. Remember that an archiving path is only relevant if not using dynamic paths for archiving. If specified as, for example, *ArchivePath1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.

- ***OldRecordingsNewPath[optional number]***
  Lets you specify what to do with old recordings in case *RecordingPath* or *ArchivePath* have been changed. If this parameter is not specified, default behavior is *Leave* (see the following). If specified as, for example, *OldRecordingsNewPath1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device. Valid options are: *Delete* (deletes old recordings), *Leave* (leaves old recordings for offline investigation but unavailable for online system), or *Move* (moves old recordings to archive).
- ***OldRecordingsNewMac[optional number]***
  Lets you specify what to do with old recordings in case a new MAC address has been specified for the hardware device. If this parameter is not specified, default behavior is Leave (see the following). If specified as, for example, *OldrecordingsNewMac1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device. Valid options are: Delete (deletes old recordings), Leave (leaves old recordings for offline investigation but unavailable for online system), or Inherit (renames all old recording folders according to the new MAC address, thus making them available for the online system).
- ***RetentionTime[optional number]***
  Required retention time (in minutes). Remember that retention time is the total of recording time plus archiving time. If specified as, for example, *RetentionTime1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***MjpegLiveFrameRate[optional number]***
  Required MJPEG live frame rate (in number of frames; depending on what has been configured on the camera, it will then know whether it is frames per second, minute, or hour). If specified as, for example, *MjpegLiveFrameRate1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***MjpegRecordingFrameRate[optional number]***
  Required MJPEG recording frame rate (in number of frames; depending on what has been configured on the camera, it will then know whether it is frames per second, minute, or hour). If you need to specify a value which includes a decimal separator, use the full stop character (example: 7.62). If specified as, for example, *MjpegRecordingFrameRate1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***MotionSensitivity[optional number]***
  A value between 0-256; corresponds to using the *Sensitivity* slider when configuring motion detection settings in the Management Application. If specified as, for example, *MotionSensitivity1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***MotionDetectionThreshold[optional number]***
  A value between 0-10000; corresponds to using the *Motion* slider when configuring motion detection settings in the Management Application. If specified as, for example, *MotionDetectionThreshold1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***MotionDetectionInterval[optional number]***
  Lets you specify how often motion detection analysis should be carried out on video from the camera. Specified in milliseconds. The interval is applied regardless of the camera's frame rate settings. If specified as, for example, *MotionDetectionInterval1*, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- ***ServerName***
  Name with which the RC-P will appear when listed in clients. Name must be unique, and must not contain any of the following special characters: < > & ' " \ / : * ? | [ ]
- ***ServerPort***
  Port number to use for communication between the RC-P server and clients.
- ***OnlineVerification***
  If this parameter is used, all online hardware devices found using *HardwareOldMacAddress* are updated. All other hardware devices are not updated. Any character means “yes, use online verification.”

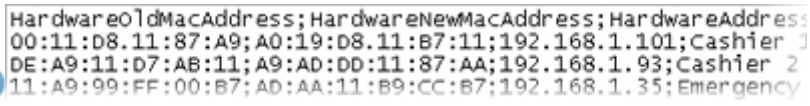
Existing configuration parameters that are not specified in CSV file will remain unchanged. If a parameter value for an individual camera in the CSV file is empty, the existing parameter value will remain unchanged on that camera.

Most system integrators store hardware device information in spreadsheets like Microsoft Excel, from which they can save the information as comma-separated values in a CSV file. These examples show hardware information in Excel (1) and when exported to a CSV file (2); note the header lines:

1

	A	B	C	
1	HardwareOldMacAddress	HardwareNewMacAddress	HardwareAddress	Came
2	00:11:D8.11:87:A9	A0:19:D8.11:B7:11	192.168.1.101	Cashi
3	DE:A9:11:D7:AB:11	A9:AD:DD:11:87:AA	192.168.1.93	Cashi
4	11:A9:99:FF:00:B7	AD:AA:11:B9:CC:B7	192.168.1.35	Emer

2



Whichever method is used, the following applies:

- The first line of the CSV file must contain the headers, and subsequent lines must contain information about one hardware device each
- Separators can be commas, semicolons or tabs, but cannot be mixed
- All lines must contain valid values—pay special attention to the fact that camera names, user names, etc. must be unique, and must not contain any of the following special characters: < > & ' " \ / : * ? | [ ]
- There is no fixed order of values, and optional parameters can be omitted entirely
- Boolean fields are considered true unless set to 0, false or no
- Lines containing only separators are ignored
- Empty lines are ignored
- Even though the CSV file format is generally ASCII only, Unicode identifiers are allowed; even without Unicode identifiers, the entire file or even individual characters are allowed to be Unicode strings

If you need to include separator characters in a value—for example if a camera name is Reception; Camera 1—you can encapsulate the value in quotes to indicate that the separator should not be interpreted as separating values in the file. Such quote-encapsulated values are interpreted as they appear. If a separator, a quote or a space is needed in a value, the whole value has to be encapsulated in quotes. Leading and trailing spaces outside the quote-encapsulated value are removed, while spaces inside the quote-encapsulated value are maintained. No characters (except spaces) are allowed outside the quote-encapsulated value. A double quote inside a quote-encapsulated value is interpreted as a single quote. Nested quotes (quotes inside quotes) are not allowed.

Some examples (using semicolon as the separator):

- "camera"; is interpreted as camera
- "cam;""era"; is interpreted as cam;"era
- """camera"""; is interpreted as "camera"
- ""; is interpreted as an empty string
- ...; " cam"" era " ;... is interpreted as | cam" era | (where the character | is not part of the interpretation but only used to show the start and end of the interpretation)
- ""camera; is not valid as there are characters outside the quote-encapsulated value
- "cam" "era"; is not valid as the two quotes are separated with a space and quotes cannot be nested
- "cam"er"a"; is not valid as you cannot nest quotes
- cam"era"; is not valid as there are characters outside the quotes

Daylight Savings Time

Daylight savings time (DST, also known as summer time) is the practice of advancing clocks in order for evenings to have more daylight and mornings to have less. Typically, clocks are adjusted forward one hour sometime during the spring season and adjusted backward sometime during the fall season, hence the saying *spring forward, fall back*. Note that use of DST varies between countries/regions.

When working with a surveillance system, which is inherently time-sensitive, it is important to know how the system handles DST.

Spring: Switch from Standard Time to DST

The change from standard time to DST is not much of an issue since you jump one hour forward. Typically, the clock jumps forward from 02:00 standard time to 03:00 DST, and the day thus has 23 hours. In that case, there is simply no data between 02:00 and 03:00 in the morning since that hour, for that day, did not exist.

Fall: Switch from DST to Standard Time

When you switch from DST to standard time in the fall, you jump one hour back. Typically, the clock jumps backward from 02:00 DST to 01:00 standard time, repeating that hour, and the day thus has 25 hours. In that case, you will reach 01:59:59, then immediately revert back to 01:00:00. If the system did not react, it would essentially re-record that hour, so the first instance of, for example, 01:30 would be overwritten by the second instance of 01:30.

Because of this, RC-P will forcefully archive the current video in the event that the system time changes by more than five minutes. The first instance of the 01:00 hour will not be viewable directly from clients. However, the data is recorded.

Stability Improvement

Microsoft Windows 32-bit operating systems can address 4 GB of virtual memory. The operating system kernel reserves 2 GB for itself, and each individual running process is allowed to address another 2 GB. This is Windows' default setting, and for the vast majority of RC-P installations it works fine.

The main components of the server—the Recording Server service and the Image Server service—have been compiled with the LARGEADDRESSAWARE flag. This means you can optimize the memory usage of RC-P's Recording Server and Image Server services by configuring your 32-bit Windows operating system so that it restricts the kernel to 1GB of memory, leaving 3GB of address space for processes compiled with the LARGEADDRESSAWARE flag.

This should improve the stability of especially the Recording Server service by allowing it to exceed the previous 2 GB virtual memory limit, making it possible for it to use up to 3 GB of memory. The change in Windows configuration is known as 3 GB switching.

- ## When Is 3 GB Switching Relevant?

  For very large RC-P installations and/or for installations with many megapixel cameras it can be relevant to change Windows' settings so that only 1 GB of virtual memory is reserved for the operating system kernel, leaving 3 GB for running processes.

  If using Windows' default setting, with only 2 GB virtual memory reserved for running processes, it has been seen that the Recording Server service in very large installations of RC-P may:

  - Behave erratically if getting very close to the 2 GB virtual memory limit. Symptoms can include database corruption, and client-server or camera-server communication errors.

  - Become unstable and crash if exceeding the 2 GB virtual memory limit. During such crashes, the code managing the surveillance system databases is not closed properly, and databases will become corrupt. In case of a crash, Windows will normally restart the Recording Server service. However, when the Recording Server service is restarted, one of its first tasks will be to repair the databases. The database repair process can in some cases take several hours, depending on the amount of data in the corrupted databases.

  If you experience such problems, and you run RC-P 6.5a or newer, making Windows use 3 GB for running processes is likely to solve the problems.

  If you have not experienced such problems, but you run RC-P 6.5a or newer and your RC-P installation is very large and/or features many megapixel cameras, 3 GB switching is likely to help prevent the problems from occurring.

  The way to configure 32-bit Windows to be LARGEADDRESSAWARE depends on your type of Windows operating system. In the following, you will see two methods outlining Microsoft's recommended procedure for increasing the per-process memory limit to 3 GB. Use the first method if running Windows XP Professional or Windows Server 2003. Use the second method if running Windows 2008 Server, Windows Vista Business, Windows Vista Enterprise or Windows Vista Ultimate.

- ## What to Do: If Running Windows XP Professional or Windows Server 2003

  IMPORTANT: Improper modification of boot.ini can render the operating system inoperable. On-Net Surveillance Systems, Inc. does not assume any responsibility for changes you make to the operating system.

  ### Adding the 3 GB Switch

  The following technique can be used to add the 3 GB switch to the boot.ini file. From a command prompt, enter the following to add the 3 GB switch to the end of the first line of the operating system section in the boot.ini file (requires administrative privileges):

  ```
  BOOTCFG /RAW "/3GB" /A /ID 1
  ```

  Where

  - */RAW* specifies the operating system options for the boot entry. The previous operating system options will be modified.

- *"/3GB"* specifies the 3 GB switch.
- */A* specifies that the operating system options entered with the /RAW switch will be appended to the existing operating system options.
- */ID* specifies the boot entry ID in the OS Load Options section of the boot.ini file to add the operating system options to. The boot entry ID number can be obtained by performing the command *BOOTCFG /QUERY* (this displays the contents of the boot.ini file) at the command prompt.

A reboot is required after editing the boot.ini file for the changes to take effect.

Removing the 3 GB Switch

If you want to undo the 3 GB switch mentioned above, follow this procedure:

Select *Start* > *Control Panel*, and double-click the *System* icon. Select the *Advanced* tab, and click the *Settings* button in the *Startup and Recovery* section. Click the *Edit* button in the *System Startup* section. The boot.ini file will launch in an editor. Remove the *"/3GB"* from the end of the appropriate boot entry line under the [operating systems] section. Save and close the file. Click *OK* in the *Startup and Recovery* section.

A reboot is required after editing the boot.ini file for the changes to take effect.

- ### What to Do: If Running Windows 2008 Server or Windows Vista

IMPORTANT: Improper modification of the operating system boot entry can render the operating system inoperable. On-Net Surveillance Systems, Inc. does not assume any responsibility for changes you make to the operating system.

Adding the 3 GB Switch

Select *Start* > *All Programs* > *Accessories*, right-click *Command Prompt*, and select *Run as administrator*, then click *Continue*.
Enter the following command to add the 3 GB switch to the current operating system boot entry:

```
BCDEDIT /SET INCREASEUSERVA 3072
```

Where

- *USERVA* Specifies an alternate amount of user-mode virtual address space for operating systems.
- *3072* Specifies 3 GB (3072 MB).

A reboot is required after editing the boot configuration data store for the changes to take effect.

Removing the /3GB Switch

Select *Start* > *All Programs* > *Accessories*, right-click *Command Prompt*, and select *Run as administrator*, then click *Continue*. Enter the following command to remove the 3 GB switch from the current operating system boot entry:

```
BCDEDIT /DELETEVALUE INCREASEUSERVA
```

A reboot is required after editing the boot configuration data store for the changes to take effect.

Protect Recording Databases from Corruption

In the Management Application you can select which action to take if a camera database becomes corrupted. The actions include several database repair options. While being able to select such actions is highly valuable, it is of course even better to take steps to ensure that your camera databases do not become corrupted:

- ### Power Outages: Use a UPS

The single biggest reason for corrupt databases is the surveillance system server being shut down abruptly, without files being saved and without the operating system being closed down properly. This may happen due to power outages, due to somebody accidentally pulling out the server's power cable, or similar.

The best way of protecting your surveillance system server from being shut down abruptly is to equip your surveillance system server with a UPS (Uninterruptible Power Supply).

The UPS works as a battery-driven secondary power source, providing the necessary power for saving open files and safely powering down your system in the event of power irregularities. UPSs vary in sophistication, but many UPSs include software for automatically saving open files, for alerting system administrators, etc.

Selecting the right type of UPS for your organization's environment is an individual process. When assessing your needs, however, do keep in mind the amount of runtime you will require the UPS to be able to provide if the power fails; saving open files and shutting down an operating system properly may take several minutes.

- ### Windows Task Manager: Be Careful when Ending Processes

  When working in Windows Task Manager, be careful not to end any processes which affect the surveillance system. If you end an application or system service by clicking *End Process* in the Windows Task Manager, the process in question will not be given the chance to save its state or data before it is terminated. This may in turn lead to corrupt camera databases.

  Windows Task Manager will typically display a warning if you attempt to end a process. Unless you are absolutely sure that ending the process will not affect the surveillance system, make sure you click the *No* button when the warning message asks you if you really want to terminate the process.

- ### Hard Disk Failure: Protect Your Drives

  Hard disk drives are mechanical devices, and as such they are vulnerable to external factors. The following are examples of external factors which may damage hard disk drives and lead to corrupt camera databases:

  - Vibration (make sure the surveillance system server and its surroundings are stable)
  - Strong heat (make sure the server has adequate ventilation)
  - Strong magnetic fields (avoid)
  - Power outages (make sure you use a UPS; see more information in the previous)
  - Static electricity (make sure you ground yourself if you are going to handle a hard disk drive).
  - Fire, water, etc. (avoid)

Users

Overview of Users and Groups

To get an overview of your RC-P system's users, expand *Advanced Configuration* in the Management Application's navigation pane, then expand *Users*.

The term *users* primarily refers to users who are able to connect to the surveillance system through their clients. You can configure such users in two ways:

- As **basic users**, authenticated by a user name/password combination.
- As **Windows users**, authenticated based on their Windows login

You can add both types of users through the Configure User Access wizard or individually (see Add Basic Users and Add Windows Users).

By grouping users, you can specify rights for all users within a **group** in one step. If you have many users performing similar tasks, this can save you significant amounts of work. User groups are logical groups created and used for practical purposes in the Management Application only. They are not in any way connected with user groups from central directory services such as, for example, Active Directory®. If you want to use groups, make sure you add groups before you add users: You cannot add existing users to groups.

Finally, the **administrator** is also listed under *Users*. If required, this lets you configure password protection for the Management Application.

Configure User Access Wizard

The Configure User Access wizard helps you quickly configure clients' access to the RC-P server as well as which users should be able to use clients.

When using the wizard, all users you add will have access all to cameras, including any new cameras added at a later stage. If this is not acceptable, specify access settings, users and user rights separately; see Configure Server Access. Also note that you cannot add users to groups through the wizard.

The wizard is divided into a number of pages:

- Server Access Settings
- Basic and Windows Users
- Access Summary

Add Basic Users

When adding a basic user, you create a dedicated surveillance system user account with basic user name and password authentication for the individual user. Note that adding the user as a Windows user will provide better security.

If you want to include users in groups, make sure you add required groups before you add users: You cannot add existing users to groups.

You can add basic users in two ways: One is through the Configure User Access Wizard, the other is described here:

1. In the Management Application's navigation pane, expand *Advanced Configuration*, right-click *Users*, and select *Add New Basic User*.
2. Specify a user name. User names must be unique, and must not contain the following characters: < > & ' " \ / : * ? | [ ]

   Then specify a password, and repeat it to be sure you have specified it correctly.
3. Click *OK*.

4. Specify General Access and Camera Access properties. These properties will determine the rights of the user.
5. Click *OK*
6. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

Add Windows Users

When adding Windows users, you import users defined locally on the server and authenticate them based on their Windows login. This generally provides better security than the basic user concept, and is the recommended method.

If you want to include users in groups, make sure you add required groups before you add users: You cannot add existing users to groups.

You can add Windows users in two ways: One is through the Configure User Access Wizard, the other is described here:

The users you want to add must have been defined as local PC users on the server. Simple file sharing must be disabled on the server. To disable simple file sharing, right-click Windows' *Start* button and select *Explore*. In the window that opens, select the *Tools* menu, then select *Folder Options...*, then the *View* tab. Scroll to the bottom of the tab's *Advanced Settings* list, and make sure that the *Use simple files sharing* check box is cleared. When ready, click *OK* and close the window.

1. In the Management Application's navigation pane, expand *Advanced Configuration*, right-click *Users*, and select *Add New Windows User*. This will open the *Select Users or Groups* dialog.

   Note that you will only be able to make selections from the local computer, even if you click the *Locations...* button.
2. In the *Enter the object names to select* box, type the required user name(s), then use the *Check Names* feature to verify that the user name(s) you have entered are correct. If typing several user names, separate each name with a semicolon. Example: *Rich; Matthew; Marc; Ari*
3. When ready, click *OK*.
4. Specify General Access and Camera Access properties. These properties will determine the rights of the user.
5. Click *OK*
6. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

Example of a correctly specified user name: USER001. Example of an incorrectly specified user name: PC001/USER001. The user should of course still specify a password and any required server information.

Add User Groups

User groups are logical groups created and used for practical purposes in the Management Application only. They are not in any way connected with user groups from central directory services such as, for example, Active Directory®.

By grouping users, you can specify rights for all users within a group in one step. If you have many users performing similar tasks, this can save you significant amounts of work.

Make sure you add groups before you add users: You cannot add existing users to groups.

1. In the Management Application's navigation pane, expand *Advanced Configuration*, *right-click Users*, and select *Add New User Group*.
2. Specify a name for the group. Group names must be unique, and must not contain the following characters: < > & ' " \ / : * ? | [ ]
3. Click *OK*.
4. Specify General Access and Camera Access properties. These properties will determine the rights of the group's future members.
5. Click *OK*

6. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

7. Now you can add users to the group: In the navigation pane, right-click the group you just created, and Add Basic Users or Add Windows Users as required.

Configure User and Group Rights

User/group rights are configured during the process of adding users/groups, see Add Basic Users, Add Windows Users and Add User Groups.

Note that you can also add basic and Windows users through the Configure User Access wizard. However, when using the wizard all users you add will have access all to cameras, including any new cameras added at a later stage.

If you at a later stage want to edit the rights of a user or group:

1. In the Management Application's navigation pane, expand *Advanced Configuration*, expand *Users*, right-click the required user or group, and select *Properties*.

2. Edit General Access and Camera Access properties. These properties will determine the rights of the user/group.

3. Click *OK*

4. Save your configuration changes by clicking the *Save Configuration* button in the Management Application's toolbar.

User Information

- ***User name*:** Only editable if the selected user is of the type basic user. Lets you edit the user name. User names must be unique, and must not contain the following characters: < > & ' " \ / : * ? | [ ]

- ***Password*:** Only editable if the selected user is of the type basic user. Lets you edit the password. Remember to repeat the password to be sure you have specified it correctly.

- ***User type*:** Non-editable field, displaying whether the selected user is of the type basic user or Windows user.

Group Information

- ***Group name*:** Lets you edit the group name. Group names must be unique, and must not contain the following characters: < > & ' " \ / : * ? | [ ]

General Access

- ***Live*:** Ability to view *Live video* in the Ocularis Client or Ocularis Client Lite.

- ***Playback*:** Ability to view video in *Browse mode* in the Ocularis Client or Ocularis Client Lite.

- ***Setup*:** Ability to view the *Setup* tab in Ocularis Client Lite.

- ***Edit shared views*:** Ability to create and edit views in shared groups in Ocularis Client Lite. Views placed in shared groups can be accessed by every user. If a user/group does not have this right, shared groups will be protected, indicated by a padlock icon in Ocularis Client Lite.

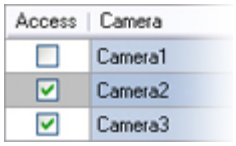
- ***Edit private views*:** Ability to create and edit views in private groups in Ocularis Client Lite. Views placed in private groups can only be accessed by the user who created them. If a user/group does not have this right, private groups will be protected, indicated by a padlock icon in Ocularis Client Lite. Denying users the right to create their own views may make sense in some cases; for example in order to limit bandwidth use.

For more information about shared and private views, see the separate *Ocularis Client User Manual* documentation

Camera Access

In the list of cameras, use the *Access* column to select which cameras the user/groups should have access to. Note the last item in the list, *Rights for new cameras when added to the system*, with which you can allow the user/group access to any future cameras.

Then, for each camera, use the *Camera* column to select the camera, and then specify which features the user/group should have access to when working with the selected camera.



Example: The user/group should have access to cameras 2 and 3. Camera 2 (note the darker background) is selected for specification of features.

Tip: If the same features should be accessible for several cameras, you can select multiple cameras by pressing SHIFT or CTRL on your keyboard while selecting.

The features are listed in two columns in the lower part of the window: the left column lists features related to live viewing, the right column lists features related to playback:

In the *Live* column, the following features, all selected by default, are available:

- ***Live*:** Ability to view live video from the selected camera(s).
    - ***PTZ*:** Ability to use navigation features for PTZ (Pan/Tilt/Zoom) cameras. A user/group will only be able to use this right if having access to one or more PTZ cameras.
    - ***PTZ Preset Positions*:** Ability to use navigation features for moving a PTZ camera to particular preset positions. A user/group will only be able to use this right if having access to one or more PTZ cameras with defined preset positions.
    - ***Output*:** Ability to activate output (lights, sirens, door openers, etc.) related to the selected camera(s).
    - ***Events*:** Ability to use manually trigger events related to the selected camera(s).
    - ***Incoming audio*:** Ability to listen to incoming audio from microphones related to the selected camera(s).
    - ***Manual recording*:** Ability to manually start recording for a fixed time (defined by the surveillance system administrator).

In the *Playback* column, the following features, all selected by default, are available:

- ***Playback*:** Ability to play back recorded video from the selected camera.
    - ***AVI/JPEG Export*:** Ability to export evidence as movie clips in the AVI format and as still images in the JPEG format.
    - ***Sequences*:** Ability to use the *Sequences* feature when playing back video from the selected camera.
    - ***Audio*:** Ability to listen to recorded audio from microphones related to the selected camera(s).

Why can I not select certain features? Typically because the selected camera does not support the features. For example, you can only select PTZ-related features if the camera is a PTZ camera. Also, some of the features depend on the user's/group's General Access properties: For example, in order have access to PTZ or output features, the user/group must have access to viewing live video; in order to use AVI/JPEG export, the user/group must have access to playing back recorded video.

Why are some feature check boxes filled with squares? Square-filled check boxes can appear in the lower part of the window if you have selected several cameras and a feature applies for some but not all of the cameras. Example: For camera A you have selected that use of the *Events* is allowed; for camera B it is not allowed. If you select both camera A and camera B in the list, the *Events* check box in the lower part of the window will be square-filled. Another example: Camera C is a PTZ camera for which you have allowed the *PTZ preset positions* feature; camera D is not a PTZ camera. If you select both camera C and camera D in the list, the *PTZ preset positions* check box will be square-filled.

Drivers

Update Video Device Drivers

Video device drivers are small programs used for controlling/communicating with the camera devices connected to the RC-P system. Video device drivers are installed automatically during the initial installation of your RC-P system. However, new versions of video device drivers—called Device Packs—are released and made available for free on the OnSSI website from time to time.

We recommend that you always use the latest version of video device drivers. When updating video device drivers, there is no need to remove the old video device drivers first; simply install the latest version on top of any old version you may have.

IMPORTANT: When you install new video device drivers, your system will not be able to communicate with camera devices from the moment you begin the installation until the moment installation is complete and you have restarted the Recording Server service. Usually, the process takes no longer than a few minutes, but it is highly recommended that you perform the update at a time when you do not expect important incidents to take place.

1. On the RC-P server on which you want to install the new video device drivers version, shut down any running surveillance software, including any running Recording Server service.

2. Double-click the downloaded video device driver file *DeviceInstaller.exe* to begin installation.

   Depending on your security settings, one or more Windows security warnings may appear after you click the link. If such security warnings appear, accept security warnings by clicking the *Run* button (button may have other name; exact button name depends on your operating system version).

3. Select required language, and click *OK*. This will open the *Video Device Driver Setup Wizard*, which will guide you through the installation. Click the *Next* button and follow the wizard.

4. When the wizard is complete, remember to start the Recording Server service again.

Hardware Driver IDs

If using the Add Hardware Devices Wizard's Import from CSV File option, you must—if cameras and server are offline—specify a *HardwareDriverID* for each hardware device you want to add. In the following, IDs for all hardware devices supported at the time of release of this version of RC-P are listed. The list is sorted alphabetically by device, with the corresponding ID at the end of each line. Example: *ACTi ACD-2100 105* indicates that you should use *105* as the ID if adding an ACTi ACD-2100 hardware device.

This list is for guidance only; IDs are subject to change without notice. More devices may be supported by the time you read this, as new versions of video device drivers—called Device Packs—are released at regular intervals. To view a current list of IDs, view the release notes for the Device Pack used in your organization. Alternatively visit the OnSSI website for the latest information.

360 Vision IP Dome 320
ACTi ACD-2100 105
ACTi ACD-2200 173
ACTi ACD-2300 152
ACTi ACD-2400 228
ACTi ACM-1011 105
ACTi ACM-1100 series 105
ACTi ACM-1230 series 105
ACTi ACM-1310 series 105
ACTi ACM-1430 series 105
ACTi ACM-1511 105
ACTi ACM-3001 105
ACTi ACM-3011 105
ACTi ACM-3100 series 105
ACTi ACM-3210 series 105
ACTi ACM-3300 series 105
ACTi ACM-3400 series 105
ACTi ACM-3511 105
ACTi ACM-3701 105
ACTi ACM-4000 series 105
ACTi ACM-4100 series 105
ACTi ACM-4200 series 105
ACTi ACM-5001 105
ACTi ACM-5600 series 105
ACTi ACM-5711 105
ACTi ACM-7400 series 105
ACTi ACM-7511 105
ACTi ACM-8100 series 105
ACTi ACM-8200 series 105
ACTi CAM-5100H 105
ACTi CAM-5100M 105
ACTi CAM-5100S 105
ACTi CAM-5120 105
ACTi CAM-5130 105
ACTi CAM-5140 105
ACTi CAM-5150 105
ACTi CAM-5200 series 105
ACTi CAM-5220 series 105
ACTi CAM-5300 series 105
ACTi CAM-5320 series 105
ACTi CAM-5500 105
ACTi CAM-5520 105
ACTi CAM-6100 105
ACTi CAM-6110 105
ACTi CAM-6120 105
ACTi CAM-6200 105
ACTi CAM-6210 105
ACTi CAM-6220 105
ACTi CAM-6230 105
ACTi CAM-6500 105
ACTi CAM-6510 105
ACTi CAM-6520 105
ACTi CAM-6600 105
ACTi CAM-6610 105
ACTi CAM-6620 105
ACTi CAM-6630 105
ACTi CAM-7100-series 105
ACTi CAM-7200-series 105
ACTi CAM-7300-series 105
ACTi SED-2100R 105
ACTi SED-2100S 105
ACTi SED-2120/2120T 105
ACTi SED-2130 105
ACTi SED-2140 105
ACTi SED-2200 105
ACTi SED-2300Q 117
ACTi SED-2310Q 117
ACTi SED-2320Q 117
ACTi SED-2400 105
ACTi SED-2410 141
ACTi SED-2420 141
ACTi SED-2600 152

ACTi SED-2610 152
ACTi TCM-4301 327
ACTi TCM-5311 334
Adam 6050 129
Adam 6060 108
Adam 6066 108
AgileMesh 100 145
American Dynamics VideoEdge Dome 157
American Dynamics VideoEdge IP Box Camera 157
APPRO LC-7224 series 156
APPRO LC-7226 series 157
Apro Technology H1000 series 255
Arecont AV1300 140
Arecont AV1305 140
Arecont AV1355 140
Arecont AV2100 140
Arecont AV2105 140
Arecont AV2155 140
Arecont AV3100 140
Arecont AV3105 140
Arecont AV3130 140
Arecont AV3155 140
Arecont AV5100 140
Arecont AV5105 140
Arecont AV5155 140
Arecont AV8180 154
Arecont AV8185 154
Arecont AV8360 154
Arecont AV8365 154
AXIS 200+ 1
AXIS 205 15
AXIS 206 19
AXIS 206M 19
AXIS 206W 19
AXIS 207 18
AXIS 207MW 18
AXIS 207W 18
AXIS 209FD 168
AXIS 209MFD 168
AXIS 210 18
AXIS 210A 18
AXIS 211 18
AXIS 211A 18
AXIS 211M 18
AXIS 211W 18
AXIS 212 PTZ 138
AXIS 213 PTZ 22
AXIS 214 PTZ 123
AXIS 215 PTZ 123
AXIS 215 PTZ-E 123
AXIS 216FD 122
AXIS 216MFD 122
AXIS 221 25
AXIS 223M 153
AXIS 225FD 25
AXIS 231D 23
AXIS 231D+ 23
AXIS 232D 23
AXIS 232D+ 23
AXIS 233D 23
AXIS 240 2
AXIS 240Q 16
AXIS 241Q 16
AXIS 241QA 16
AXIS 241S 17
AXIS 241SA 17
AXIS 242S IV 17
AXIS 243Q 160
AXIS 243SA 17
AXIS 247S 172
AXIS 282 130
AXIS 2100 5
AXIS 2110 5
AXIS 2120 6
AXIS 2130 12
AXIS 2400 OSYS 3
AXIS 2400 Linux 8
AXIS 2400+ 8
AXIS 2401 OSYS 4
AXIS 2401 Linux 11
AXIS 2401+ 11
AXIS 2411 14
AXIS 2420 10
AXIS 2420 10
AXIS M1011 283
AXIS M1031 284
AXIS M3011 285
AXIS M3014 342
AXIS M7001 286
AXIS P1311 288
AXIS P3301 246
AXIS P3343 339
AXIS P3344 339
AXIS Q1755 278
AXIS Q6032 335
AXIS Q7401 256
AXIS Q7404 337
AXIS Q7406 268
Barix Barionet 272
Basler BIP-640c 242
Basler BIP-640c-dn 242
Basler BIP-1000c 242
Basler BIP-1000c-dn 242
Basler BIP-1300c 242
Basler BIP-1300c-dn 242
Basler BIP-1600c 242
Basler BIP-1600c-dn 242
Baxall X-Stream 91
Bosch Dinion NWC-0455-10P 133
Bosch Dinion NWC-0495-10P 133
Bosch FlexiDome NWD-0455 133
Bosch FlexiDome NWD-0495 133
Bosch VideoJet X10 253
Bosch VideoJet X20 253
Bosch VideoJet X40 253
Bosch VIP X1 127
Bosch VIP X2 132
Bosch VIP X1600 162
Bosch VG4 Series 190
Canon VB-C10 31
Canon VB-C50FSi 212
Canon VB-C50i 212
Canon VB-C50iR 212
Canon VB-C60 276
Canon VB-C300 174
Canon VB-C500 330
CBC Ganz ZN-D2024 207
CBC Ganz ZN-PT304L 179
CBC Ganz ZN-PT304WL 179
Checkview 9128702 275
Cisco IPC-2500 322
Cisco IPC-4300 322
Cisco IPC-4500 322
Convision S1 21
Convision V100 21
Convision V200 20
Convision V6xx 7
Convision V7xx 7
D-Link DCS1000/1000W 55
D-Link DCS-2000 101
D-Link DCS-2100+/2100/2100G 101
D-Link DCS-3220/3220G 118
D-Link DCS-5300 99
D-Link DCS-5300G 99
D-Link DCS-6620/6620G 116
Darim Vision PVE400 298
Digimerge DNB6320 177
Digimerge DND7220 177
Digimerge DNP5220E 177
Digimerge DNP5320E 177
Digimerge DNS1010 177
Digimerge DNZ-9320W 244
DirectShow camera 214
Discrete DIV2300 188
DvTel DVT-7101 262
DvTel DVT-7608 261
DvTel DVT-9460 514
DvTel DVT-9540DW 514
Dynacolor Diva Standard 296
Dynacolor Diva Zoom 282
Dynacolor Diva Mini 297
Etrovision EV3130 236
Etrovision EV3131 237
Etrovision EV3131A 237
Etrovision EV3830 238
Etrovision EV6130 239
Etrovision EV6230 240
Etrovision EV6530 240
Extreme CCTV EX7 103
Extreme CCTV EX30 103
Extreme CCTV EX36 103
Extreme CCTV EX80 103
Extreme CCTV EX82 103
Extreme CCTV EX85 140
Extreme CCTV REG-L1-IP 103
Eyeview CMI-110 245
Eyeview CMI-H230 245
Eyeview CMI-H260 245
Eyeview EYENET-250A 245
Eyeview GPOWER IP Basement 245
Eyeview IPM-100 245
Eyeview IPM-150 245
Eyeview IPM-300 245
Eyeview IPM-500 245
Eyeview IPR-220 245
Eyeview IPR-330 245
Eyeview IPR-6000 245
Eyeview IPR-6600 245
Eyeview IPS-110 245
Eyeview IPS-220 245
Eyeview IPS-300 245
Eyeview IPS-330 245
Eyeview IPS-400 245
Eyeview IPS-500 245
Eyeview IPS-600 245
Eyeview IPS-800 245
Eyeview IPS-830 245
Eyeview IPS-900 245
FLIR 241S 95
GE Security GEC-IP2B 225
GE Security GEC-IP2B-C 225
GE Security GEC-IP2B-P 225
GE Security GEC-IP2D 225
GE Security GEC-IP2D-C 225
GE Security GEC-IP2D-P 225
GE Security GEC-IP2VD 225
GE Security GEC-IP2VD-C 225
GE Security GEC-IP2VD-P 225
GE Security GEC-IP2VD-DN 225
GE Security GEC-IP2VD-DNC 225
GE Security GEC-IP2VD-DNP 225
Grandeye Halocam IPC 249
Grandeye Halocam IPW 249
HikVision DS6101 277
HikVision DS6104 273
Hitron HECMC4V4C4 217
Hitron HEV0104 223
Hitron HEV0407 224
Hitron HNCA-811-NZ1 222
Hitron HNCB-811NZ1 219
Hitron HNCB-F1SN 218
Hitron HNCG-F1SAW0S4 220
Hitron HNCV-811PZ0S4 221

Hitron HWD-12SMP 187
Hunt HLC-81I 201
Hunt HLC-81M 201
Hunt HLC-83M 202
Hunt HLC-83V 203
Hunt HLT-86F 198
Hunt HLT-87Z 209
Hunt HLV-1CI 200
Hunt HLV-1CM 200
Hunt HVT-01HT 199
Hunt HWS-01HD 204
Hunt HWS-04HD/W 205
ICanServer 510 257
ICanServer 512 257
ICanServer 540 259
ICanView 220 258
ICanView 222 258
ICanView 230 258
ICanView 232 258
ICanView 240 257
ICanView 250 257
ICanView 260 258
ICanView 270 257
ICanView 280 258
ICanView 290 257
Infinova V1700N-C series NetDome 119
Infinova V1700N-L series NetDome 137
Intellinet MNC-L10/550710 104
ioibox series 400
ioibox series 401
ioicam series 400
IPIX IS2000/CVD2000/CVN2000 57
IPIX CVD3000 57
Ipx DDK-1000 157
Ipx DDK-1500 157
Ipx DDK-1500D 157
Ipx VE-3500 157
IQEye101 83
IQEye300 series 83
IQEye 4 series 83
IQEye501 83
IQEye510 83
IQEye 511 83
IQEye600 series 83
IQEye700 series 83
IQEye800 Sentinel series 83
IQEye Alliance series 83
Johnson Controls DVN5008 293
JVC VN-A1U 43
JVC VN-C10U 44
JVC VN-C20U 126
JVC VN-C30U 42
JVC VN-C3WU 40
JVC VN-C205 169
JVC VN-C215 146
JVC VN-C625U 45
JVC VN-C655U 45
JVC VN-E4/-E4E /-E4U 121
JVC VN-V25 185
JVC VN-V26 185
JVC VN-V225 185
JVC VN-V685 196
JVC VN-V686/V686B 196
JVC VN-V686WPC 196
JVC VN-X35 235
JVC VN-X235 235
Lenel ICT-220 345
Lenel ICT-230 345
Lenel ICT-250 346
Lenel ICT-510 345
Lenel LC-330FDX 345
Linudix LWS800 511
Linudix LWS820 512
Linudix LWS840 511
Lumenera LE165 84
Lumenera LE175 84
Lumenera LE256 84
Lumenera LE259 84
Lumenera LE275 84
Lumenera LE375 84
Lumenera LE575 84
Mobotix D10 86
Mobotix D12 86
Mobotix D22M 86
Mobotix M1 86
Mobotix M10 86
Mobotix M12 86
Mobotix M22M 86
Mobotix Q22 260
Mobotix Q24 328
Optelecom Siqura BC-2x series 281
Optelecom Siqura C-50 269
Optelecom Siqura C-54 289
Optelecom Siqura C-60 321
Optelecom Siqura FD-2x series 281
Optelecom Siqura S-50 269
Optelecom Siqura S-54 289
Optelecom Siqura S-60 321
Optelecom Siqura V-30 295
Panasonic BB-HCE481 series 24
Panasonic BB-HCM311 series 24
Panasonic BB-HCM331 series 24
Panasonic BB-HCM371A 24
Panasonic BB-HCM381 series 24
Panasonic BB-HCM403 24
Panasonic BB-HCM511 180
Panasonic BB-HCM515 180
Panasonic BB-HCM527 180
Panasonic BB-HCM531 180
Panasonic BB-HCM547 180
Panasonic BB-HCM580 180
Panasonic BB-HCM581 180
Panasonic BB-HCS301 24
Panasonic BL –C1 series 24
Panasonic BL-C10 series 24
Panasonic BL-C20 series 24
Panasonic BL-C30 series 24
Panasonic BL-C111 182
Panasonic BL-C131 182
Panasonic KX-HCM8 63
Panasonic KX-HCM10 series 63
Panasonic KX-HCM110A series 24
Panasonic KX-HCM230 series 63
Panasonic KX-HCM250 series 63
Panasonic KX-HCM270 series 63
Panasonic KX-HCM280 series (except 280A) 63
Panasonic KX-HCM280A 24
Panasonic WJ-NT104 60
Panasonic WJ-NT304 183
Panasonic WV- NF284 120
Panasonic WV-NF302 211
Panasonic WV-NP240/WV-NP244 120
Panasonic WV-NP304 211
Panasonic WV-NP472 61
Panasonic WV-NP502 351
Panasonic WV-NP1000/WV-NP1004 120
Panasonic WV-NS202 143
Panasonic WV-NS320 series 64
Panasonic WV-NS950 197
Panasonic WV-NS954 197
Panasonic WV-NW470 85
Panasonic WV-NW484 175
Panasonic WV-NW502 351
Panasonic WV-NW960 197
Panasonic WV-NW964 197
Pentax Versacam IC-4 50
Pelco Camclosure IP series 149
Pelco Endura Net5301T 144
Pelco Endura Net5308T 166
Pelco Endura Net5316T 167
Pelco IP3701 176
Pelco NET300 208
Pelco NET350 208
Pelco Spectra IV-IP 213
Pelco SpectraMini IV-IP 213
Philips NETSVR-1 93
Philips NETSVR-6 92
Pixord 120 72
Pixord 126 75
Pixord 200 73
Pixord 201 73
Pixord 205 77
Pixord 207 77
Pixord 24X 74
Pixord 261 78
Pixord 1000 75
Pixord 400/400W 151
Pixord 461 148
Pixord 463 148
Pixord 1401/1401W 136
Pixord 2000 76
Pixord 4000 151
Polar Industries zPan100 501
Provideo SD-606W 279
Provideo SD-705VPRO-1 280
Samsung SCC-C6475 131
Samsung SHR-2040 165
Samsung SNC-B2315 227
Samsung SNC-B5395 248
Samsung SNC-C6225 325
Samsung SNC-C7225 325
Samsung SNC-C7478 299
Samsung SNC-M300 226
Samsung SNT-1010 147
Samsung Techwin SNC550 191
Samsung Techwin SNC570 291
Samsung Techwin SND460V 329
Samsung Techwin SND560 292
Samsung Techwin SNP1000/SNP1000A 195
Samsung Techwin SNP3300/SNP3300A 194
Samsung Techwin SNS100 192
Samsung Techwin SNS400 193
Sanyo VCC-400N 206
Sanyo VCC-9500 206
Sanyo VCC-9500P 206
Sanyo VCC-9600 206
Sanyo VCC-9600P 206
Sanyo VCC-9700 206
Sanyo VCC-9700P 206
Sanyo VCC-9800 206
Sanyo VCC-9800P 206
Sanyo VCC-HD4000 206
Sanyo VCC-HD4000P 206
Sanyo VCC-HDN1(S) 206
Sanyo VCC-N6584 206
Sanyo VCC-N6695P 206
Sanyo VCC-WB2000/VCC-WB4000 56
Sanyo VCC-P450 206
Sanyo VCC-P450NA 206
Sanyo VCC-P470 206
Sanyo VCC-P470NA 206
Sanyo VCC-P7574 142
Sanyo VCC-P7575P 142
Sanyo VCC-P9574 142
Sanyo VCC-P9574N 142
Sanyo VCC-P9575P 142
Sanyo VCC-PN9575P 142

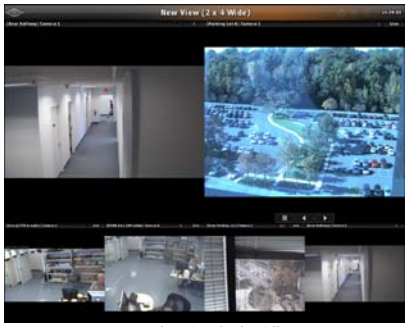
Sanyo VCC-PT490 206
Sanyo VCC-PT490NA 206
Sanyo VCC-PT500 206
Sanyo VCC-PT500NA 206
Sanyo VCC-XZ200 206
Sanyo VCC-XZ200P 206
Sanyo VCC-XZ600P 206
Sanyo VCC-XZN600P 206
Sanyo VCC-ZM600P 206
Sanyo VCC-ZMN600P 206
Sanyo VDC-DP7584 142
Sanyo VDC-DP7585P 142
Sanyo VDC-DP9584 142
Sanyo VDC-DP9584N 142
Sanyo VDC-DP9585 142
Sanyo VDC-DPN9585P 142
Sanyo VSP-SV2000 56
Siemens CCIC1345 252
Siemens CCIS1345 252
Siemens CCIS1345-DN 252
Siemens CCIW1345 252
Sony SNC-CS3 54
Sony SNC-CS10 88
Sony SNC-CS11 88
Sony SNC-CS20 216
Sony SNC-CS50 125
Sony SNC-CM120 215
Sony SNC-DF40 88
Sony SNC-DF50 178
Sony SNC-DF70 88
Sony SNC-DF80 178
Sony SNC-DF85 178
Sony SNC-DM110 215
Sony SNC-DM160 215
Sony SNC-DS10 216
Sony SNC-DS60 216
Sony SNC-M1/SNC-M1W 102
Sony SNC-M3/SNC-M3W 102
Sony SNC-P1 88
Sony SNC-P5 98
Sony SNC-RX530 124
Sony SNC-RX550 124
Sony SNC-RX570 124
Sony SNC-RZ25 89
Sony SNC-RZ30 52
Sony SNC-RZ30/2 52
Sony SNC-RZ50 128
Sony SNC-Z20 53
Sony SNC-VL10 51
Sony SNT-V304 9
Sony SNT-V501 82
Sony SNT-V704 113
Speco Technologies SIPB1/SIPB2 501
Speco Technologies SIPB3/SIPB4 501
Speco Technologies SIPMPT5 501
Speco Technologies SIPSD10X 501
StarDot NetCam XL 186
StarDot NetCam SC 5 MP 186
Toshiba IK-WB01A 115
Toshiba IK-WB02A 114
Toshiba IK-WB15A 115
Toshiba IK-WB11A 59
Toshiba IK-WB21A 115
Toshiba IK-WD01A 508
Toshiba IK-WR01A 114
Toshiba Teli CI7010 181
Toshiba Teli CI8110D 263
Toshiba Teli CI8210D 250
Toshiba Teli EJ7000 170
UDP IPC1100 231
UDP IPC3100 231
UDP IPC3500 231
UDP IPC4100 229
UDP IPC4500 229
UDP NVE12K 230
UDP NVE40K 230
UDP NVE100 232
UDP NVE1000 233
UDP NVE2000 234
UDP NVE4000 230
Universal driver 400
Universal driver 16 Chnl. 401
Vantage VIPC1100E 501
Vantage VIPC1311EP 501
Vantage VIPC1431EP 501
Vantage VIPC3100E 501
Vantage VIPC3211EP 501
Vantage VIPC3311EP 501
Vantage VIPC5300 501
Vantage VIPC5320 501
Vantage VIPC6510F 501
Vantage VIPC6610F 501
Vantage VIPC7100 series 501
Vantage VIPC7200 series 501
Vantage VIPC7300 series 501
Vantage VIPS2120 501
Vantage VIPS2310Q 501
Vantage VIPS2410 506
VCS VideoJet 10 96
VCS VideoJet 400 94
VCS VIP 10 96
Veo Observer XT 32
Verint Nextiva S1700e 103
Verint Nextiva S1704e 135
Verint Nextiva S1708e 111
Verint Nextiva S1712e 163
Verint Nextiva S1724e 164
Verint Nextiva S1900e 103
Verint Nextiva S1950e 103
Verint Nextiva S1970e 103
Verint Nextiva S2600e/S2610e 103
Verint Nextiva S2700e 103
Videology 20N758 184
Videology 21N758 184
Videology Server Board 189
Vivotek FD6100 series 109
Vivotek FD7131 331
Vivotek FD7132 331
Vivotek FD7141 331
Vivotek FD7141V 331
Vivotek IP2121 58
Vivotek IP2122 58
Vivotek IP3121 97
Vivotek IP3122 97
Vivotek IP3135 97
Vivotek IP6124 109
Vivotek IP7130 333
Vivotek IP7131 155
Vivotek IP7133 348
Vivotek IP7134 348
Vivotek IP7135 155
Vivotek IP7137 155
Vivotek IP7138 331
Vivotek IP7139 331
Vivotek IP7142 251
Vivotek IP7151 251
Vivotek IP7152 251
Vivotek IP7153 251
Vivotek IP7154 251
Vivotek IP7160 251
Vivotek IP7161 251
Vivotek IP7251 347
Vivotek IP7330 333
Vivotek IZ7151 349
Vivotek PT3124 107
Vivotek PT7135 158
Vivotek PT7137 158
Vivotek PZ6122 110
Vivotek PZ7111 332
Vivotek PZ7112 332
Vivotek PZ7121 332
Vivotek PZ7122 332
Vivotek PZ7131 332
Vivotek PZ7132 332
Vivotek PZ7151 349
Vivotek PZ7152 349
Vivotek SD6122V 110
Vivotek SD7151 338
Vivotek SD7313 338
Vivotek SD7323 338
Vivotek VS2101 58
Vivotek VS2402 68
Vivotek VS2403 0
Vivotek VS3100 97/107
Vivotek VS3102 97/107
Vivotek VS7100 251
WebEye E10 50
Xview AP-400/Linudix 81

Ancillary Applications

Ocularis Client

Users view RC-P surveillance system video using the Ocularis Client via Ocularis Base.

- With **Ocularis Client**, users:
  - May monitor live video from an unlimited number of cameras at multiple sites
  - Have instant investigation capabilities
  - Can easily access and investigate alerts generated by motion or external systems
  - Export video clips and still images for further event handling or as court evidence



Example: Ocularis Client

NVR Download Manager

Using the NVR Download Manager

The NVR Download Manager lets you manage which RC-P-related features your organization's users will be able to access from a targeted welcome page on the surveillance system server. You access the NVR Download Manager from Windows' *Start* menu: Select *All Programs* > *NVR Download Manager*.

- #### Examples of User-Accessible Features

  - **The Ocularis Client**. With a browser, users connect to the surveillance server where they are presented with a welcome page. From the welcome page, users may download the **Ocularis Client** software and install it on their computers.

  - **Various plugins**. Downloading such plugins can be relevant for users if your organization uses add-on products with the RC-P solution.

- #### What Does the Welcome Page Look Like?

  The welcome page is a simple web page with links to downloading or running various features. It is available in a number of languages; users select their required language from a menu in the top right corner of the welcome page.

  To view the welcome page, simply open an Internet Explorer browser (version 6.0 or later) and connect to the following address:

  http://[surveillance server IP address or hostname]

  If the Image Server service has been configured with a port number other than the default port 80 (you configure this as part of the server access properties), users must specify the port number as well, separated from the IP address or hostname by a colon:

  http://[surveillance server IP address or hostname]:[port number]

The content of the welcome page is managed through the NVR Download Manager; therefore the welcome page will often look different in different organizations.

Initial Look

The initial look of the welcome page is automatically provided through the NVR Download Manager's default configuration—for more information, see *Default Configuration of Download Manager.*

- ## Default Configuration of Download Manager

The NVR Download Manager has a default configuration. This ensures that your organization's users can access standard features without the surveillance system administrator having to set up anything.

The NVR Download Manager's configuration is represented in a tree structure.

The fact that only standard features are initially available—and only in the same language version as the surveillance system itself—helps reduce installation time and save space on the server. There is simply no need to have a feature or language version available on the server if nobody is going to use it.

You can, however, easily make more features and/or languages available as required. See *Making New Features Available* in the following for more information.

- ## Making New Features Available

Making new features—including new language versions—available to your organization's users involves two procedures: First you install the required features on the surveillance system server. You then use the NVR Download Manager to fine-tune which features should be available in the various language versions of the welcome page.

Installing New Features on Server

If the NVR Download Manager is open, close it before installing new features on the server.

To install a feature from the *Installers* folder, select the required language sub-folder, then double-click the required installation (.exe) file.

When a new feature has been installed on the surveillance system server, you will see a confirmation dialog. If required, you can open the NVR Download Manager from the dialog.

Making New Features Available through the Download Manager

When you have installed new features—such as language packs, etc.—by default, they will be selected in the NVR Download Manager, and thus immediately be available to users via the welcome page.

You can always show or hide features on the welcome page by selecting or clearing check boxes in the NVR Download Manager's tree structure.

- ## Hiding and Removing Features

You can remove features in several ways:

- You can **hide features** from the welcome page by clearing check boxes in the NVR Download Manager's tree structure. In that case, the features will still be installed on the surveillance system server, and by selecting check boxes in the NVR Download Manager's tree structure you can quickly make the features available again.

- You can **remove features** which have previously been made available through the NVR Download Manager. This will remove the installation of the features on the surveillance system server. The features will disappear from the NVR Download Manager, but installation files for the features will be kept in the surveillance system server's installers folder, so you can re-install them later if required.

    1. In the NVR Download Manager, click the *Remove features...* button.
    2. In the *Remove Features* window, select the features you want to remove
    3. Click *OK*. You will be asked to confirm that you want to remove the selected features. If you are sure, click the *Yes* button.

- You can **remove installation files for non-required features** from the surveillance system server. This can help you save disk space on the server if you know that your organization is not going to use

certain features—typically non-relevant language versions. See Remove Installation Files for End-User Features for more information.

- ## Virus Scanning Information

  If you are using virus scanning software on the RC-P server, it is likely that the virus scanning will use a considerable amount of system resources on scanning data from the NVR Download Manager. If allowed in your organization, disable virus scanning on all or parts of the RC-P server. For more information see Virus Scanning Information.

Recording Server Manager

Using the Recording Server Manager

The Recording Server service is a vital part of the surveillance system; video streams are only transferred to RC-P while the Recording Server service is running. The Recording Server Manager informs you about the state of the Recording Server service. It also lets you manage the service.

In the notification area (a.k.a. system tray), the Recording Server Manager's icon indicates whether the Recording Server service is running or not. Green indicates running (default), red indicates not running.

By right-clicking the icon you can start and stop the Recording Server service, view log files, etc.:

- ### Start the Recording Server Service

  1. Right-click the notification area's Recording Server icon.
  2. In the menu that appears, select *Start Recording Server Service.*
  3. The icon in the notification area changes to green.

- ### Stop the Recording Server Service

  1. Right-click the notification area's Recording Server icon.
  2. In the menu that appears, select *Stop Recording Server Service.*
  3. The icon in the notification area changes to red.

- ### Open the Management Application

  1. Right-click the notification area's Recording Server icon.
  2. In the menu that appears, select *Open Management Application.*

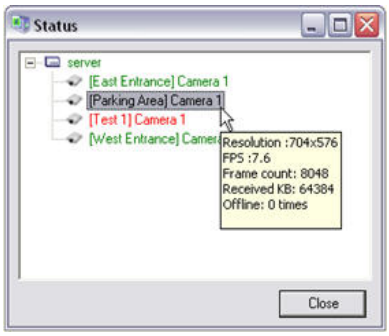
- ### Monitor System Status

  By right-clicking the notification area's Recording Server icon and then selecting *Show System Status*, you get access to the *Status* window.

  The *Status* window lets you view the status of the image server(s) and connected cameras. The status of each server/camera is indicated by a color:

  - ***Green*** indicates that the server or camera is running correctly.
  - ***Gray*** indicates that the *camera* (not the server) is not running. Typically, a camera will be indicated in gray in the following situations:
    - the camera is not online (as defined in the camera's online period schedule).
    - the Recording Server service has been stopped.
  - ***Red*** indicates that the server or camera is not running. This may because it has been unplugged or due to a network or hardware error. Errors are listed in the Recording Server log file.

  Place your mouse pointer over a camera in the status window to view details about the camera in question. The information updates approximately every 10 seconds.



- ***Resolution*:** The resolution of the camera.
- ***FPS*:** The number of frames per second (a.k.a. frame rate) currently used by the camera. The number updates each time the camera has received 50 frames.
- ***Frame count*:** The number of frames received from the camera since the Recording Server service was last started.
- ***Received KB*:** The number of kilobytes sent the by camera since the Recording Server service was last started.
- ***Offline*:** Indicates the number of times the camera has been offline due to an error.

- ## View the Recording Server Service Log File

1. Right-click the notification area's Recording Server icon.
2. In the menu that appears, select *Open Recording Server Log File....*

For more information about log files, see Configure Audit, Event & System Logging.

- ## View the Image Server Service Log File

1. Right-click the notification area's Recording Server icon.
2. In the menu that appears, select *Open Image Server Log File....*

For more information about log files, see Configure Audit, Event & System Logging.

- ## Access the Built-in Help System

1. Right-click the notification area's Recording Server icon.
2. In the menu that appears, select *Help*.

For more information, see Use the Built-in Help System.

- ## View Version Information

Knowing the exact version number can be useful in case you require support from OnSSI.

1. Right-click the notification area's Recording Server icon.
2. In the menu that appears, select *About...*

- ## Exit the Recording Server Manager

1. Right-click the notification area's Recording Server icon.
2. In the menu that appears, select *Exit Recording Server Manager.*

> **Tip:** If you later want to re-open the Recording Server Manager, go to Windows' Start menu and select *All Programs > Startup > Recording Server Manager*.

Ocularis Viewer

The Ocularis Viewer is a stand alone application that allows users to view video clips exported from Ocularis Client. The exported video is in Ocularis database format.

The Ocularis Viewer allows users to:

- View and playback video clips exported from Ocularis Client
- Export additional clips from the original clip
- Export still images from the original clip
- Print reports based on images in the original clip

The Ocularis Viewer is installed automatically on the same machine as the Ocularis Client. It may also be included as part of a video export for users who do not have Ocularis Client but need to view the exported video.

For more information on the Ocularis Viewer, see the *Ocularis Viewer User Manual* available from www.onssi.com.

Backup

System Configuration Backup

We recommend that you make regular backups of your RC-P configuration (cameras, schedules, views, etc.) as a disaster recovery measure. While it is rare to lose your configuration, it can happen under unfortunate circumstances. Luckily, it takes only a minute to back up your existing configuration.

The following describes backup of the configuration in RC-P version 1.0.

In the following, we assume that you have not changed RC-P's default configuration path, which is *C:\Documents and Settings\All Users\Application Data\OnSSI*\RC-P on servers running Windows® XP or Windows Server 2003, and *C:\Program Data\OnSSI*\RC-P on servers running all other supported operating systems. If you have changed the default configuration path, you must take your changes into consideration when using the method described in the following.

To Back Up:

1. If RC-P is used on a server running Windows XP or Windows Server 2003, make a copy of the folder *C:\Documents and Settings\All Users\Application Data\OnSSI\RC-P* and all of its sub-folders.

   If RC-P is used on a server running any other supported operating system, make a copy of the folder *C:\Program Data\OnSSI*\RC-P and all of its sub-folders.

2. Open the folder *C:\Program Files\Onssi\RC-P\devices*, and verify if the file *devices.ini* exists. If the file exists, make a copy of it. The file will exist if you have configured video properties for certain types of cameras; for such cameras, changes to the properties are stored in the file rather than on the camera itself.

3. Store the copies away from the RC-P server, so that they will not be affected if the server is damaged, stolen or otherwise affected.

   Remember that a backup is a snapshot of your RC-P system configuration at the time of backing up. If you later change your configuration, your backup will not reflect the most recent changes. Therefore, back up your system configuration regularly.

To Restore Your Backed-up Configuration:

1. If RC-P is used on a server running Windows XP or Windows Server 2003, copy the content of the backed-up *RC-P* folder into *C:\Documents and Settings\All Users\Application Data\OnSSI*\RC-P.

   If RC-P is used on a server running any other supported operating system, copy the content of the backed-up *RC-P* folder into *C:\Program Data\OnSSI*\RC-P

2. If you backed up the file *devices.ini*, copy the file into *C:\Program Files\OnSSI\RC-P\devices*

Removal

Entire System

Remove Entire Surveillance System

To remove the entire RC-P surveillance system (that is the surveillance server software and related installation files and video device drivers) from your server, do the following:

What happens to recordings? Your recordings will not be removed; they will remain on the server even after the server software has been removed. Likewise, the RC-P configuration file will remain on the server; this allows you to reuse your configuration if you later install RC-P again.

1. Shut down all RC-P components.
2. In Windows' *Start* menu, select *Control Panel*, and select *Add or Remove Programs*.
3. In the *Add or Remove Programs* window's list of currently installed programs, select the *RC-P **system*** entry (not the *RC-P* entry) and click the *Change/Remove* button.
4. The setup wizard appears; click the *Next* button, then the *Remove* button.
5. Select *Remove entire surveillance system*, then click *Next*, and complete the wizard's remaining steps.

Individual Components

Remove Installation Files for End-User Features

When you have installed RC-P, your surveillance system server contains installation files for a number of end-user features by default. The installation files lets you install the end-user features on the surveillance system server, and make them available to your organization's users through the Download Manager.

You can remove installation files for non-required features from the surveillance system server. This can help you save disk space on the server if you know that your organization is not going to use certain features, for example non-relevant language versions:

1. Open the *Installers* folder located in the RC-P installation folder, typically at C:\Program Files\OnSSI\RC-P\Installers.
2. Select the required language sub-folder, then delete the unwanted installation (.exe) files.

Remove the NVR Download Manager

To remove the NVR Download Manager separately from the other RC-P surveillance server software:

1. In Windows' *Start* menu, select *Control Panel*, and select *Add or Remove Programs*.
2. In the *Add or Remove Programs* window's list of currently installed programs, select *NVR Download Manager*.
3. Click the *Remove* button.

Remove the Surveillance Server Software

To remove the RC-P server software (not including the Download Manager or the Ocularis Client), do the following:

What happens to recordings? Your recordings will not be removed; they will remain on the server even after the server software has been removed. Likewise, the RC-P configuration file will remain on the server; this allows you to reuse your configuration if you later install RC-P again.

1. Shut down all RC-P components.
2. In Windows' *Start* menu, select *Control Panel*, and select *Add or Remove Programs*.
3. In the *Add or Remove Programs* window's list of currently installed programs, select the *RC-P* entry (not the *RC-P **system*** entry) and click the *Remove* button.

4. You will be asked to confirm that you want to remove RC-P. If you are sure that you want to remove the software, click *OK*.

    - If a *Status Information* window appears on your screen during installation, simply click its *OK* button (the window simply provides a summary of what has been removed).

5. Click *Finish*.

Remove Video Device Drivers

Video device drivers are small programs used for controlling/communicating with the camera devices connected to an RC-P system. To remove the video device drivers, do the following:

1. Open Windows' *Control Panel*, and select *Add or Remove Programs*.

2. In the *Add or Remove Programs* window, select the *Video Device Pack Vx.x* entry (where *x.x* indicates the version number), and click the *Remove* button.

3. You will be asked to confirm that you want to remove the video device drivers. If you are sure, click *OK* .

Contact Information

On-Net Surveillance Systems (OnSSI)

One Blue Plaza
7th Floor
P.O. Box 1555
Pearl River, NY 10965

Website:	www.onssi.com	
General:	info@onssi.com	845.732.7900
Fax:		845.732.7999
Sales Support:	sales@onssi.com	845.732.7900 x 1
PreSales Support	salesengineering@onssi.com	845.732.7900 x 2
Technical Support:	support@onssi.com	845.732.7900 x 3
Training:	training@onssi.com	845.732.7900 x 4
Marketing:	marketing@onssi.com	845.732.7900 x 5